931/.12
4-1

Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

fortgeführt von

C. W. Borchardt, K. Weierstrass, L. Kronecker,
L. Fuchs, K. Hensel, L. Schlesinger

gegenwärtig herausgegeben von

Helmut Hasse und **Hans Rohrbach**

unter Mitwirkung von

W. Brödel, M. Deuring, O. Haupt,
G. Köthe, W. Schmeidler

Band 195

In 4 Heften

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung / J. Guttentag, Verlagsbuchhandlung / Georg Reimer / Karl J. Trübner / Veit & Comp.

Berlin 1955

MATH
NMI
J8264
v. 195-198

Archiv-Nr. 180355
Satz von Walter de Gruyter & Co., Berlin W 35
Druck von Buchkunst, Berlin W 35
Printed in Germany

Apr. 22, 1958
B.T.

Inhaltsverzeichnis des Bandes 195

Seite

Aigner, Alexander, Die kubische Fermatgleichung in quadratischen Körpern 3

— —, Einige Sätze über Lagebeziehungen in endlichen Graphen 18

— —, Unmöglichkeitskernzahlen der kubischen Fermatgleichung mit Primfaktoren der Art $3n + 1$ 175

Ballier, Friedhorst, Über lineartopologische Algebren 42

Beyer, Gudrun, Erweiterungsproblem galoisscher Körper und Zerfall einfacher Algebren 215

Carlitz, L. und **John H. Hodges,** Distribution of bordered symmetric, skew and hermitian matrices in a finite field 192

Eichler, Martin, Zur Zahlentheorie der Quaternionen-Algebren 127

— —, Über die Darstellbarkeit von Modulformen durch Thetareihen . . . 156

Evans, Arwel, A note on continued fractions and dimension theory 102

Fréchet, Maurice, La paraanalitikaj funkcioj en n dimensioj 22

Halberstam, H., Über additive zahlentheoretische Funktionen 210

Hodges, John H. siehe **Carlitz, L.**

Kanold, Hans-Joachim, Über zahlentheoretische Funktionen 180

Klein-Barmen, Fritz, Multiplikative Funktionen über euklidischen und Sternverbänden 121

Knödel, Walter, Primzahldifferenzen 202

Rieger, G. J., Zum Waringschen Problem für algebraische Zahlen und Polynome 108

Sade, A., Sur le problème des transvasements 1

Stöhr, Alfred, Bemerkungen zur additiven Zahlentheorie. III 172

Tillmann, Heinz Günther, Dualität in der Funktionentheorie auf Riemannschen Flächen 76

Volkmann, Bodo, Ein Satz über die Menge der vollkommenen Zahlen 152

Ausgabedaten der Hefte von Bd. 195

Heft 1/2 ausgegeben am 30. November 1955

Heft 3/4 ausgegeben am 31. Januar 1956

Sur le problème des transvasements.

Par *A. Sade* à Marseille.

Ce problème, signalé pour la première fois par N. Chuquet (Triparty, 1484), puis par Tartaglia au 16° s. peut s'énoncer ainsi: On a trois vases A, B, C contenant en tout s unités de volume. La capacité de A est quelconque, mais au moins égale à s. Les capacités de B et C sont p et q; $(s > p > q)$ p et q sont premiers entre eux. Soit i le contenu initial, f le contenu final de B. Comment passer de i à f par des transvasements? Bachet (Problèmes délectables, 1624, p. 206) traite la question pour $s = 8$, $p = 5$, $q = 3$, $i = 0$, $f = 4$. V. Etten (1626), Ougthred (1653), Ozanam (1694), Labosne (1879) imitent cette solution. H. Schubert (1895) étudie le cas $i = 0$, $s = kf$. Brunel (1895) dénombre les solutions qui repassent plusieurs fois par le même état. R. Sprague (1940) exprime la condition de possibilité au moyen d'une suite de Farey. Sawyer (1950) et Mingot Shelly (1951) considèrent des cas particuliers.

Dans le présent travail on se propose 1° de donner un critère de possibilité ne conduisant pas à des calculs pratiquement inabordables, 2° d'indiquer le nombre des transvasements nécessaires.

u, v, w étant les contenus respectifs de A, B, C à un moment quelconque, on peut faire correspondre à cet état le point de coordonnées cartésiennes u, v, w. Alors, en posant $D = p + q - s$, les points accessibles par des transvasements, dont le nombre est $2(p + q)$ si $D \leqq 0$ et $p + q + s$ si $D > 0$, sont situés sur le périmètre d'un parallélogramme déterminé (qui peut être tronqué) et l'on peut passer de tout «point» de ce contour au «point» du même contour déduit du premier par une translation parallèle à un des côtés du périmètre. Les points consécutifs ainsi définis sont les sommets d'un polygone.

A chaque polygone correspond un cycle de restes dont la loi de formation est la suivante: Le terme qui suit v est $s - v$ ou $v + q$ (mod p) suivant que v est supérieur ou non à $s - q = h$.

Pour que l'on puisse passer par transvasements de $v = i$ à $v = f$ et vice versa il faut et il suffit que i et f appartiennent au même cycle. Pour que l'on puisse passer seulement de i à f il faut et il suffit que f appartienne au même cycle que 0.

Le cas $D \leqq 1$ est banal. Si $D > 1$, chaque cycle contient soit un, soit deux termes m, m' supérieurs à h, et qui le caractérisent. Le nombre total des cycles est $E\left(\frac{D+1}{2}\right)$, $D \geqq 3$. En groupant dans une même classe tous les cycles du même ordre on obtient trois classes au plus. Les cycles d'une même classe se déduisent les uns des autres de la façon suivante: Soient m, m' les deux éléments supérieurs à h figurant dans un même cycle. On majore d'une unité le terme m et tous ceux qui précèdent m et suivent m'. On diminue d'une unité m' et tous les termes qui précèdent m' et suivent m. Ou on fait la même opération à rebours. Dans cette transformation la différence $k = m' - m$ ne peut dépasser un certain maximum, e, propre à la classe considérée. Chaque classe est

engendrée par l'un des nombres $E(s/2)+1$, $E[(s-p)/2]+1$, $E[(s-q)/2]+1$. Il existe une première classe, contenant l'élément $m=h+1$; elle est engendrée par le terme $q-1$. La derniere classe (qui peut coïncider avec la précédente) contient l'élément $m=p-1$; elle est engendrée par le terme $s-p+1$. Il peut exister une classe intermédiaire. Quand la différence $m'-m$ est paire, la classe correspondante se termine par un cycle d'ordre moitié de l'ordre des cycles de cette classe. Ce cycle ne contient qu'un élément supérieur à h; il peut aussi être regardé comme engendré par l'un des trois nombres: $(s-q)/2$, $s/2$, $(s-p)/2$. Si l'on compte ce cycle terminal comme faisant partie de la classe et si e est la différence maxima, $m-m'$, pour cette classe, celle-ci contient $E(e/2)+1$ cycles. Une classe peut se réduire à son cycle terminal.

Le problème des transvasements étant ainsi ramené à celui de reconnaître si deux nombres i et f, appartiennent ou non au même cycle, et chaque cycle étant caractérisé par son, ou ses deux termes m, m', supérieurs à h, tout revient à chercher si le cycle qui contient i et le cycle qui contient f ont, ou non, un nombre m supérieur à h commun. D'après la loi de formation des cycles on est conduit à trouver la plus petite valeur entière, positive, de x pour laquelle $i+qx$ donne un reste (mod p) supérieur à h, ce qui peut se noter: $i+qx>h \pmod p$.

Pour résoudre la congruence $ax+b>c \pmod d$, *où a et d sont premiers entre eux,*

1°) *si* $c<d-a$ *et* $a+b<d$,

résoudre l'inégalité ordinaire $ax+b>c$ *et choisir pour x la plus petite valeur entière positive* ($\neq 0$) *satisfaisant à cette inégalité*;

2°) *si* $c<d-a$ *et* $d\leqq a+b$,

résoudre de la même manière l'inégalité ordinaire: $ax+b>c+d$;

3°) *si* $c\geqq d-a$,

chercher la plus petite valeur positive ($\neq 0$) *de y pour laquelle*

$$(*)\qquad dy-b<d-c;\ dy-b\neq 0 \pmod a.$$

Quand y est connu, x est le quotient entier, non nul, de $dy-b$ par a. Si le reste, r, non nul, est retranché de d, on aura (à titre de vérification): $ax+b=d-r \pmod d$.

4°) *Si l'on aboutit à $r=0$, ou à $x=0$, il faut prendre la 2me valeur de y qui satisfait* (*) (*la 3me si les deux cas se succèdent*).

On a une règle analogue pour $ax+b<c \pmod d$. Les valeurs successives $d, d', \ldots, a, a', \ldots$ qui apparaissent dans les congruences diminuant comme dans la recherche du PGCD de a et de d, on finit par aboutir à une congruence évidente.

Exemple. $s=14295456$, $p=7155529$, $q=7145679$, $h=7149783$. Est-il possible de passer de $i=143859$ à $f=1129459$? Dans le cycle engendré par i cherchons le premier élément qui surpasse h. Il faut résoudre successivement:

$$7145673\,x+143859>7149783 \pmod{7155529}$$
$$9856\,x+7011670<5746 \pmod{7155529}$$
$$73\,y+5802>4110 \pmod{9856}$$

d'où $y=1$, $x=15$, $m=7151548$.

Pour savoir si f appartient au même cycle que i il faut résoudre $qx+f>h \pmod p$ dont la solution est: $x'=115$, $m=7151548$, comme pour i.

On peut donc passer de i à f et de f à i par des transvasements et il y a $x'-x=100$ termes dans la suite des contenus successifs du 2° vase, qui relie i à f.

Eingegangen 28. Juli 1953.

Die kubische Fermatgleichung in quadratischen Körpern.

Von *Alexander Aigner* in Graz.

1. Einleitung und Übersicht.

In zwei früheren Arbeiten[1]) widmete ich mich der Gleichung $x^3 + y^3 = z^3$, welche in $K(\sqrt{m})$ und $K(\sqrt{-3m})$ zugleich lösbar oder unlösbar ist. Sie ist im besonderen unlösbar für $m < 0$, $m \equiv 2(3)$ mit nicht durch 3 teilbarer Klassenzahl des Körpers (nach Fueter 1913), ferner auch für $m > 0$, $m \equiv 1(3)$ bei nicht durch 3 teilbarer Klassenzahl von $K(\sqrt{-3m})$. Wegen dieser Koppelung zwischen m und $-3m$ genügt es übrigens, *m nicht durch 3 teilbar* zu nehmen, was wir künftig auch stets tun wollen.

Nun zeigte sich bei diesem Problem aber eine gewisse Wendung; und zwar von der Klassenzahl zu restcharakterlichen Eigenschaften der Primteiler der Zahl m. Erstlinig der kubische Charakter von 2, zweitlinig der quadratische Charakter bestimmter Zahlen aus $K(\sqrt{2})$, so etwa der Grundeinheit, sind hier von Bedeutung.

Die vorliegende Arbeit bringt nun einige weitere Resultate in dieser Richtung, vor allem aber einen Einblick in die so eigenartige Struktur des Problems, die damit zutage tritt. Die prinzipielle Möglichkeit oder Unmöglichkeit der Titelgleichung richtet sich nach dem von allfälligen Faktoren mit 2 als kubischem Nichtrest befreiten Teil der Zahl m. Setzt man $m = \pm R \cdot k$, wobei R höchstens nur Faktoren mit 2 als kubischem Nichtrest enthält (auch $R = 1$), so gibt es derartige „freie Teile" k, für die die Gleichung stets unmöglich wird, und zwar unabhängig von der Klassenzahl. Eine solche Zahl k will ich *Unmöglichkeitskernzahl*, kurz *Kernzahl* nennen. (Sie ist sozusagen ein Kern der Unlösbarkeit, denan sich beliebig Faktoren mit 2 als kubischem Nichtrest anlagern können.) Die von ihr ausgehende Reihe der Zahlen $\pm Rk$ heiße *Kernkette*.

Für Zahlen, die nicht auf einer Kernkette liegen, deren freier Teil also kein Kern ist, bleibt die Möglichkeit der Titelgleichung prinzipiell offen, wobei sie aber (schon wegen der Klassenzahl) nicht immer eintritt. — Dabei ist, streng genommen, die Kernzahl nur als eine solche definiert, für die nach den hier entwickelten Methoden die Unlösbarkeit der Titelgleichung erkannt werden kann. Theoretisch wäre es sogar möglich (wenn auch nicht anzunehmen), daß die gesamte Kette einer Nichtkernzahl lauter unlösbare Fälle liefert, diese sich also praktisch völlig wie eine Kernzahl verhält. — Nach dem Bisherigen (anfangs zitierte Arbeiten) sind 1 und $2q$, mit $q = 6n + 5$ Primzahl und $\sqrt[3]{2} - 1$ quadratischer Nichtrest mod q, solche Kernzahlen. Ich werde nun weitere Typen von Kernzahlen sowie auch von Nichtkernzahlen angeben. Als besonderes und relativ weittragendes Ergebnis bringe ich schließlich den Satz, daß *keine Kernzahl* $\equiv 2(3)$ ist.

---

[1]) *A. Aigner*, Weitere Ergebnisse über $x^3 + y^3 = z^3$ in quadratischen Körpern, Monatshefte f. Math. 56 (1952), S. 240—252 und S. 335—338.

Den Angelpunkt dieser Untersuchungen liefert die Äquivalenz von

$$(1) \quad x^3 + y^3 = z^3 \text{ in } K(\sqrt{m}) \quad \text{und} \quad X^4 + 4XY^3 = mZ^2 \text{ rational}, \ (X, Y) = 1.$$

Da sei folgende kurze Bezeichnung eingeführt: es sei

m_1 der quadratfreie Teil von $X^3 + 4Y^3$,
m_2 der quadratfreie Teil von X.

Wegen $(X, Y) = 1$, daher $(X, X^3 + 4Y^3) = 1, 2, 4$, wobei $X^3 + 4Y^3 \equiv 1(2)$ oder $\equiv 4(8)$, also m_1 ungerade ist, gilt die Zerlegung

$$m = m_1 \cdot m_2.$$

Die Primfaktoren der (quadratfreien) Zahl m verteilen sich irgendwie auf m_1 und m_2. Für Primzahlen $6n + 1$ mit 2 als kubischem Nichtrest kommt dabei natürlich nur m_2 in Betracht, wie auch für 2. — Und weil (1) auch gleichzeitige Vorzeichenänderung von X und Y zuläßt, kann man etwa $X^3 + 4Y^3 > 0$ normieren. m_1 ist damit ein *positiver ungerader* Teiler von m.

Damit führt unser Problem naturgemäß auf Untersuchungen im Körper $K(\sqrt[3]{2})$, weshalb das Wichtigste und später Benötigte über ihn hier vorangestellt sei. — Er hat die Klassenzahl 1, die Ganzheitsbasis $1, \sqrt[3]{2}, \sqrt[3]{4}$ und eine unabhängige Einheit $\varepsilon = \sqrt[3]{2} - 1$. Wir wollen seine Zahlen künftig meist mit griechischen Buchstaben bezeichnen und auch gelegentlich statt $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ kurz (abc) schreiben. Die Norm dieser Zahl ist

$$N = N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc.$$

Die „ungeraden", d. h. nicht durch $\sqrt[3]{2}$ teilbaren Körperzahlen sind die mit ungeradem a. Eine solche ist *primär*, d. h. $\equiv 1(\sqrt[3]{4})$, oder nicht, d. h. $\equiv \varepsilon(\sqrt[3]{4})$, je nachdem b gerade oder ungerade ist. Primäre und nicht primäre Zahlen gehen auseinander durch Multiplikation mit der Einheit ε hervor. — Bezüglich des quadratischen Restcharakters von ε gibt es zwei Klassen, die ich kurz mit

$$\varepsilon^+ \text{ und } \varepsilon^-$$

bezeichnen will. (Nach Primidealen der Klasse ε^+ ist ε quadratischer Rest.) Der Erklärungsmodul hierfür ist 4.

2. Der quadratfreie Faktor von $X^3 + 4Y^3$.

Wir befassen uns zunächst mit der m_1 genannten (positiven ungeraden) Zahl. Es zerfällt im Körper $K(\sqrt[3]{2})$

$$X^3 + 4Y^3 = (X + Y\sqrt[3]{4})(X^2 + 2Y^2\sqrt[3]{2} - XY\sqrt[3]{4}) = \Phi \cdot \psi;$$

beide Faktoren sind entweder teilerfremd oder haben nur den Primteiler $\sqrt[3]{2}$ gemeinsam, und dann in 2. bzw. 4. Potenz. Wegen $3 \nmid m$ und $X^3 + 4Y^3 \not\equiv 0(9)$ scheidet auch der Idealteiler von 3 aus. — Mit $X^3 + 4Y^3 > 0$ ist auch $\Phi = X + Y\sqrt[3]{4} > 0$.

Wir bezeichnen nun den quadratfreien Teil von $\Phi = (X0Y)$ mit $\alpha = (abc)$ und setzen

$$(2) \qquad X + Y\sqrt[3]{4} = (a + b\sqrt[3]{2} + c\sqrt[3]{4})(f + g\sqrt[3]{2} + h\sqrt[3]{4})^2 = \alpha \cdot \varpi^2.$$

Leicht findet man, daß $N(\alpha) = m_1$, dem quadratfreien Teil von $X^3 + 4Y^3$, ist. Zunächst ist mit $\Phi > 0$ auch $\alpha > 0$, sodann ist α „ungerade", also a ungerade; somit ist $N(\alpha)$ positiv ungerade. Ferner enthält Φ, weil die Kongruenz $\Phi \equiv 0$ genau eine rationale Wurzel für $\sqrt[3]{4}$ ergibt, zu jeder in $X^3 + 4Y^3$ aufgehenden Primzahl p nur ein Primideal ersten Grades (also weder im Falle $p = 6n + 1$ zwei solche noch im Falle $p = 6n + 5$ ein Primideal zweiten Grades); es sei denn $X \equiv Y \equiv 0(p)$, was ausdrücklich ausgeschlossen ist. Daher enthält Φ nur Primideale ersten Grades von lauter verschiedenen Normen und damit ist $N(\alpha) = m_1$.

Die Methode, alle Möglichkeiten der Gleichung (1) zu erschöpfen, besteht somit darin, für alle positiven ungeraden Teiler m_1 von m und die zugehörigen Körperzahlen α mit $N(\alpha) = m_1$ den Ansatz (2) zu machen, d. h. zu versuchen, α durch Multiplikation mit einer Quadratzahl des Körpers in eine Zahl mit verschwindendem Mittelglied $(X0Y)$ überzuführen; und sodann, falls diese Überführung überhaupt gelingt, nachzusehen, welche Werte dabei das X, bzw. sein quadratfreier Teil, annimmt, und ob der „passende" Wert $m_2 = m/m_1$ darunter vorkommen kann.

Zu einem m_1, also auch zu m, gibt es nur endlich viele wesentlich verschiedene α. — Der zunächstliegende Ansatz $m_1 = 1$, $\alpha = 1$ fällt praktisch aus, weil er allein in wiederholter Anwendung zu einem infiniten Regreß führt; $m_1 = 1$, $\alpha = \varepsilon$ ist nur für gerades m möglich und auch da nur, wenn m kein Primideal der Klasse ε^- enthält (vgl. die anfangs zitierten Arbeiten).

Der Ansatz (2) liefert nun durch Koeffizientenvergleich das System der drei Gleichungen

$$\text{(3a)} \qquad af^2 + 2bg^2 + 4ch^2 + 4cfg + 4bfh + 4agh = X$$

$$\text{(3b)} \qquad bf^2 + 2cg^2 + 2ah^2 + 2afg + 4cfh + 4bgh = 0$$

$$\text{(3c)} \qquad cf^2 + ag^2 + 2bh^2 + 2bfg + 2afh + 4cgh = Y$$

Wir haben bei gegebenen a, b, c ein passendes Tripel f, g, h zu ermitteln, so daß der mittlere Koeffizient verschwindet.

Zunächst einiges zur Teilerfremdheit. Für $(X, Y) = 1$ ist $(f, g, h) = 1$ natürlich notwendig, aber wie sich zeigen wird, auch hinreichend. (3a, b, c) ist ein lineares Gleichungssystem für die drei Werte $F = f^2 + 4gh$, $G = g^2 + 2fh$, $H = h^2 + fg$ mit der Determinante $-2N(\alpha) \neq 0$. Daher könnte $X \equiv Y \equiv 0$ ohne $F \equiv G \equiv H \equiv 0$ nur für 2 und die Primteiler von N eintreten. Nun folgt aber aus $2 \mid X, Y$ nach (3a) $2 \mid f$, dann aus (3c) $2 \mid g$, und schließlich nach (3b) auch $2 \mid h$. Die 2 spielt also keine Sonderrolle. Auch 3, der einzige Primfaktor, wo $F \equiv G \equiv H \equiv 0$ ohne $f \equiv g \equiv h \equiv 0$ möglich ist, (wegen $f : g : h \equiv 1 : \sqrt[3]{2} : -\sqrt[3]{4} \equiv \sqrt[3]{4} : \sqrt[3]{2} : 1$), kommt nach obigem $(3 \nmid m)$ nicht in Betracht.

So bleiben nur die Teiler von N; ein solcher sei $p = \lambda \cdot \mu$ mit dem Primideal 1. Grades (λ) und dem (vielleicht noch weiter zerfallenden) Faktor μ. Soll nun überhaupt $p \mid X, Y$ sein, d. h. $p \mid \Phi = \alpha\varphi^2$ mit $\lambda \mid \alpha$ (und $\mu \nmid \alpha$), so muß $\mu \mid \varphi$, also $\Phi = \alpha(\mu\beta)^2$ sein. Setzt man $X = pX'$, $Y = pY'$, $\alpha = \lambda\alpha'$, so wird $\Phi = \alpha'\lambda\mu \cdot \mu\beta^2 = p\alpha' \cdot \mu\beta^2$, also $\Phi/p = X' + Y'\sqrt[3]{4} = \alpha'\mu\beta^2$, was wieder nur so möglich ist, daß $p \mid X', Y'$ (also $p^2 \mid X, Y$, womit sich schon die ganze Gleichung durch p^6 kürzen ließe). Damit wird aber auch $\lambda \mid \alpha'\mu\beta^2$, also ($\lambda \nmid \alpha'$, weil α quadratfrei) $\lambda \mid \beta$ somit $\lambda\mu \mid \mu\beta$, d. i. $p \mid \varphi$, was soviel wie $p \mid f, g, h$ bedeutet. — Damit ist der hinreichende Charakter von $(f, g, h) = 1$ für $(X, Y) = 1$ bewiesen.

Untersuchen wir das Gleichungssystem (3a, b, c) nun noch vorerst nach dem Modul der Potenzen von 2, (wobei mit $2 \mid f$ stets $2 \nmid g$ gilt, weil φ nur $\sqrt[3]{2}$ in erster Potenz enthalten kann), so zeigt sich hier der Unterschied zwischen primär und nicht primär, sowie zwischen den Klassen ε^+ und ε^- (Kapitel 1, Schluß) mit dem Erklärungsmodul 4. Es ergeben sich für $\pm(abc)$ folgende Restsysteme:

ε^+ primär:	100, 103, 121, 122.
ε^+ nicht primär:	110, 111, 130, 131.
ε^- primär:	101, 102, 120, 123.
ε^- nicht primär:	112, 113, 132, 133.

Man kann weiter durch Multiplikation mit einer passenden Potenz von ε^2 (was auf eine Hineinziehung einer Einheit in φ hinauskommt) jede dieser 4 Klassen auf einen ihrer Vertreter normieren, etwa auf 100, 110, 102, 112.

Bezüglich der Gleichungen (3a, b) ergibt sich dann folgendes Resultat:

ε^+ primär:	(3b) möglich, $X \equiv 1(2)$ oder $\equiv 0(4)$, m beliebig.
ε^+ nicht primär:	(3b) möglich, $X \equiv 2(4)$, m gerade.
ε^- primär:	(3b) möglich, $X \equiv 1(2)$ oder $\equiv 4(8)$, m ungerade.
ε^- nicht primär:	(3b) unmöglich.

3. Der maßgebende quadratische Rest.

Nun wollen wir die Gleichung (3b) weiterhin untersuchen. Faßt man etwa f, g, h als homogene ebene Koordinaten auf, so ist es die Gleichung eines Kegelschnittes, und zwar stets eines nicht zerfallenden, da die Determinante $-2N \not\equiv 0$ ist. Wir lösen etwa nach h auf und erhalten

$$2a \cdot h = -2bg - 2cf \pm \sqrt{D},$$

wobei die Diskriminante D die Form 2. Grades in f und g

$$D = (4c^2 - 2ab)\, f^2 + 4(2bc - a^2)\, fg + 4(b^2 - ac)\, g^2$$

ist und ein Quadrat werden muß, damit wir eine (ganz) rationale Lösung erhalten. In ihren Koeffizienten sowie in den Hauptminoren 2. Ordnung der Kegelschnittsdeterminante erscheinen dieselben drei Zahlen

$$d_1 = a^2 - 2bc,\ d_2 = b^2 - ac,\ d_3 = 4c^2 - 2ab, \tag{4}$$

als Funktionen von $(abc) = \alpha$ auch mit $d_i(\alpha)$ bezeichnet ($i = 1, 2, 3$). *Keine verschwindet*; der Kegelschnitt ist keine Parabel. $d_1 \neq 0$ gilt schon, weil d_1 ungerade ist; bei $d_2 = 0$ oder $d_3 = 0$ wäre, wie eine Ausrechnung ergibt, $N(\alpha)$ ein Quadrat, während sie doch quadratfrei ist. Es sei denn $N = 1$, welcher Fall schon behandelt ist.

Eben dieselben drei Zahlen (4) treten auch als Koeffizienten der zu $\alpha = (abc)$ konjugierten Zahl (2. Grades) $\bar{\alpha} = (d_1\ \tfrac{1}{2} d_3 d_2)$ auf.

Setzen wir nun $D = k^2$, so wird

$$aNf^2 + d_2 k^2 = (fd_1 - 2gd_2)^2, \tag{5}$$

was nach Legendre genau dann rational zu lösen ist, wenn die Zahlen aN und d_2 nicht beide negativ sowie gegenseitig quadratische Reste sind. Und eine teilerfremde Lösung führt auch auf eine solche für f, g, h und damit für X, Y.

Bezüglich des *Vorzeichens* wäre nach $N > 0$, $\alpha > 0$ nur der Fall $a < 0$, $c < 0$ näher zu untersuchen. Aus $\alpha < 0$, d. h. $|b\sqrt[3]{2}| > |a| + |c\sqrt[3]{4}|$ folgt aber unmittelbar $b^2 - ac > 0$. Die Vorzeichenbedingung ist also immer erfüllt.

Bezüglich der quadratischen Reste ist nach den drei Beziehungen

$$d_1^2 - d_2 d_3 = aN, \qquad 4d_2^2 - d_1 d_3 = 2bN, \qquad \tfrac{1}{4} d_3^2 - d_1 d_2 = cN$$

stets aN quadratischer Rest nach d_2 (und d_3; analog $2bN$ und cN); ebenso sind

$$d_1, d_2, d_3 \text{ gleichzeitig quadratische Reste nach } N.$$

Sie bilden mod N die geometrische Reihe $d_2 : d_1 : d_3 \equiv 1 : \sqrt[3]{4} : \sqrt[3]{16}$.

Ferner teilt N die Zahlen $d_1^3 - 4d_2^3$ und $d_3^3 - 4d_1^3$. — Und da schließlich sicher $d_2 = b^2 - ac$ quadratischer Rest nach a ist, kommt alles auf die eine Bedingung hinaus, daß d_2 *quadratischer Rest nach N ist.* Dabei ist im Falle quadratfreier Norm N auch stets $(d_2, N) = 1$; denn ein gemeinsamer Teiler ginge in d_1, d_2, d_3 auf, also eine natürliche Zahl in der konjugierten $\bar{\alpha}$, was bei quadratfreier Norm von α unmöglich ist. — Wir erhalten demnach den wichtigen und ganz allgemein (nebenbei auch für gerades a) gültigen Satz:

Eine Zahl (abc) mit quadratfreier Norm kann genau dann durch Multiplikation mit einem Quadrat in eine Zahl ohne Mittelglied $(X\ 0\ Y)$ übergeben, wenn $b^2 - ac$ quadratischer Rest nach ihrer Norm ist.

Das ist z. B. nicht der Fall für (7 4 4) mit der Norm 55 und $b^2 - ac = -12$.

Wählen wir nun α *primär*, also b gerade, so wird

$$aN = a^4 + 2ab^3 + 4ac^3 - 6a^2bc \equiv 1\,(4), \text{ bei geradem } c \text{ sogar} \equiv 1\,(8);$$

bei ungeradem c ist aber $d_2 = b^2 - ac$ ungerade und gleich seinem ungeraden Teil u_2. Daher wird, falls $(u_2, a) = 1$ ist, direkt im Jacobischen Restsymbol

$$(d_2/N) = (d_2/aN) = (u_2/aN) = (aN/u_2) = +1.$$

Und setzt man sonst die quadratfreien Teile der Zahlen u_2, a und N (letzterer N selbst) gleich x_1x_2, $x_2x_3x_4$, x_4x_5 mit $(x_i, x_j) = 1$, so gilt auf Grund obiger Relationen $(x_2x_3x_5/x_1) = +1$ sowie

$$(x_1x_2/x_3) = (x_1x_2/x_4) \quad = (-x_1x_3x_5/x_2) \quad = +1$$

bzw.

$$(2x_1x_2/x_3) = (2x_1x_2/x_4) = (-2x_1x_3x_5/x_2) = +1,$$

wobei $x_2x_3x_5 \equiv 1\,(4)$ bzw. auch noch $\equiv 1\,(8)$ gilt. — Daraus wird nun

$$(-x_1/x_2)\,(x_2/x_1)\,(x_3x_5/x_1x_2) = (x_1x_2/x_3x_5) = +1 \text{ bzw. } (2x_1x_2/x_3x_5) = +1,$$

was schließlich $(x_1x_2/x_4x_5) = +1$ bzw. $(2x_1x_2/x_4x_5) = +1$, also jedenfalls $(d_2/N) = +1$ ergibt. Es gilt also

$$\text{(6)} \qquad \textit{Jacobisymbol}\left(\frac{d_2}{N}\right) = +1, \qquad \textit{wenn } \alpha \textit{ primär.}$$

Für primäre Zahlen ist also die maßgebende quadratische Restbedingung im Prinzip immer erfüllbar, deshalb freilich noch nicht tatsächlich erfüllt (s. obiges Beispiel); die Anzahl der Primteiler, die sie nicht erfüllen, ist gerade, wenn auch nicht notwendig Null.

Beim *Übergang zur assoziierten Zahl* $\varepsilon\alpha = (2c - a\,a - b\,b - c)$ tritt an Stelle von d_2 die Zahl

$$d_2(\varepsilon\alpha) = (a - b)^2 - (2c - a)\,(b - c) = a^2 + b^2 + 2c^2 - ab - ac - 2bc.$$

Diese Zahl ist nach dem Modul α kongruent

$$(b^2 + 2bc + 2c^2\ b^2 + bc + 2c^2\ b^2 + bc + c^2) = (1\ 1\ 1) \cdot (b^2\ bc\ c^2),$$

wovon der erste Faktor die Einheit ε^{-1}, der zweite aber mod. α kongruent $b^2 - ac = d_2$ ist. Also gilt die Beziehung

$$\text{(7)} \qquad d_2(\alpha) \equiv \varepsilon \cdot d_2(\varepsilon\alpha) \pmod{\alpha}.$$

Beim Übergang von α zu $\varepsilon\alpha$ bleibt somit der quadratische Charakter für alle Primidealteiler der Klasse ε^+ gleich, während er sich für alle solchen der Klasse ε^- ändert. Hier tritt wieder der Unterschied dieser beiden Klassen zutage. — Enthält α (mindestens) einen Teiler der letzteren Klasse, so sind jedenfalls nicht beide Ansätze $\Phi = \alpha\varphi^2$ und $\Phi = \varepsilon\alpha\varphi^2$ lösbar.

Gehört die primäre Zahl α selbst der Klasse ε^- an, enthält sie also eine ungerade Anzahl solcher Primteiler, so wird das Jacobi-Symbol für die Zahl $\varepsilon\alpha$ nach (6) und (7) gleich -1, also die maßgebende quadratische Restbedingung an sich unerfüllbar. Nichtprimäre Zahlen der Klasse ε^- sind also als quadratfreier Teil einer Zahl ohne Mittelglied unmöglich. Ein Resultat, das wir schon bei der Betrachtung des Gleichungssystems (3) mod. der Zweierpotenzen erhielten und das sich hiermit auf andere Weise bestätigt.

Lassen wir nun $N(\alpha) = p$ eine *Primzahl* sein (2 kubischer Rest) und wählen α primär, so bedeutet das Jacobisymbol $+1$ auch wirklich quadratischen Rest und somit wird $\Phi = \alpha\varphi^2$ stets möglich. Das bedeutet den Satz:

Für jede Primzahl p mit 2 als kubischem Rest ist $X^3 + 4Y^3 = pZ^2$ mit teilerfremden X, Y lösbar.

Ohne die Teilerfremdheit wäre der Satz trivial.

4. Die Gestalt des Faktors X.

Wir wenden uns jetzt der Gestalt zu, welche nach (3a) das X bzw. sein quadratfreier Teil m_2 im Falle der Lösbarkeit von (3b) annimmt. — Zu diesem Zwecke gehen wir von einer Lösung aus, deren Existenz wir wenigstens im Falle der Primzahlen nachgewiesen haben: $A + C\sqrt[3]{4} = \alpha\beta^2$ mit $(A, C) = 1$. Da läßt sich jede beliebige andere Lösung (es gibt entsprechend der Lösungsmannigfaltigkeit von (5) deren unendlich viele) in der Form

$$(X\,0\,Y) = (A\,0\,C)\quad (f\,g\,h)^2$$

wenigstens mit gebrochenen rationalen Zahlen f, g, h darstellen. Das führt wieder auf ein Gleichungssystem der Art (3a, b, c) mit $A, 0, C$ an Stelle von a, b, c. Nun ist aber — das eben als besonderer Vorteil — die mittlere Gleichung in f linear:

$$f(Ag + 2Ch) = -Cg^2 - Ah^2.$$

Die eine Möglichkeit $Ag + 2Ch = Cg^2 + Ah^2 = 0$ führt, nachdem $A, C \neq 0$ (sonst wäre der quadratfreie Faktor $\alpha = 1$, welcher Fall schon erledigt ist) und auch $A^3 + 4C^3 \neq 0$ ist, nur auf $g = h = 0$ (mit $f = 1$), also auf dieselbe Lösung A, C zurück. Für jede davon verschiedene Lösung X, Y ist somit $Ag + 2Ch \neq 0$, und wir können demnach für f in die obere Gleichung für X einsetzen und erhalten

$$(8)\qquad X(Ag + 2Ch)^2 = -3AC^2 \cdot g^4 + (4A^3 - 8C^3) \cdot g^3h + 18A^2C \cdot g^2h^2 + 24AC^2 \cdot gh^3 + (A^3 + 16C^3) \cdot h^4,$$

eine Form 4. Grades in g und h, wo wir uns bei Multiplikation mit der 4. Potenz des gemeinsamen Nenners unter g, h auch wieder ganze Zahlen vorstellen können. Es kommt also auf die algebraisch-zahlentheoretische Beschaffenheit dieses Polynoms an. — Diese Form hat auch A selbst, da die Lösung A, C aus einer anderen durch dieselbe Formel erhalten wird.

Demnach kann eine Primzahl (auch für $g \equiv h \equiv 0$) nur dann in X in ungerader Potenz, d. h. in m_2 enthalten sein, wenn sie Teiler des inhomogenen Polynomes

$$P(x) = -3AC^2x^4 + (4A^3 - 8C^3)\,x^3 + 18A^2Cx^2 + 24AC^2x + (A^3 + 16C^3)$$

mit $x = g/h$ ist. Für $g \neq 0$, $h = 0$ ergibt sich wegen $-3AC^2$ die bekannte Äquivalenz von m und $-3m$; dieser Fall darf hier beiseite bleiben. Für jeden anderen Fall ist $h \neq 0$. — Und es gibt, wie wir sehen werden, Nichtteiler dieses Polynoms.

Die algebraischen Verhältnisse liegen hier ganz gleichartig wie bei dem speziellen Polynom in meiner anfangs zitierten zweiten Arbeit. Transformiert man die Gleichung $P(x) = 0$ auf die $-3AC^2$-fachen Wurzeln und schafft das Glied mit x^3 weg, so bekommt man

$$x^4 - 6(A^3 + C^3)(A^3 + 4C^3)x^2 + 4(2A^3 - C^3)(A^3 + 4C^3)^2 x - 3(A^3 + C^3)^2 (A^3 + 4C^3)^2 = 0$$

mit der kubischen Resolvente

$$\left[z - 4(A^3 + C^3)(A^3 + 4C^3)\right]^3 + 2\left[6AC(A^3 + 4C^3)\right]^3 = 0,$$

wo die kubische Adjunktion auf $\sqrt[3]{2}$ und die letzte quadratische auf $\sqrt{A^2 + 2C^2\sqrt[3]{2} - AC\sqrt[3]{4}}$ hinausläuft. Dieser Radikand ist der konjugierte Faktor 2. Grades zu $A + C\sqrt[3]{4}$; und nachdem $(A\,0\,C) = \alpha\beta^2$ mit $\alpha = (abc)$ war, wird die konjugierte Zahl gleich $\bar{\alpha}\bar{\beta}^2$; also kommt es schließlich auf $\sqrt{\bar{\alpha}}$, die Quadratwurzel aus der zur Zahl α (mit quadratfreier Norm m_1) konjugierten Zahl

$$\bar{\alpha} = (a^2 - 2bc\; 2c^2 - ab\; b^2 - ac) = (d_1\, \tfrac{1}{2} d_3\, d_2)$$

hinaus.

Bezüglich der Kongruenzwurzeln von $P(x) = 0$ nach den Primzahlen $p > 3$ ergibt sich daraus folgendes Bild; es gibt deren 5 Arten.

1) $6n + 1$ mit 2 als kubischem Nichtrest: *eine* Kongruenzwurzel.
2) $6n + 1$ mit 2 als kubischem Rest und allen drei Werten von $\bar{\alpha}$ als quadratischem Rest: *vier* Kongruenzwurzeln.
3) $6n + 1$ mit 2 als kubischem Rest und nur einem Wert von $\bar{\alpha}$ als quadratischem Rest: *keine* Kongruenzwurzel; *Nichtteiler*.
4) $6n + 5$ mit $\bar{\alpha}$ als quadratischem Rest: *zwei* Kongruenzwurzeln.
5) $6n + 5$ mit $\bar{\alpha}$ als quadratischem Nichtrest: *keine* Kongruenzwurzel; *Nichtteiler*.

Die Teiler von m_1 selbst sind hierbei ausgenommen; ihr Verhalten als Teiler von $P(x)$ ist auch belanglos, weil sie dadurch nur gemeinsame Teiler von X und Y würden und sich aus der Grundgleichung (1) wegkürzten.

Geht man also von einer gegebenen quadratfreien Zahl $m_1 = N(\alpha)$ aus, so kann die Gleichung $X^4 + 4XY^3 = m_1 m_2 Z^2$ (wobei m_2 quadratfrei und zu m_1 teilerfremd) jedenfalls durch den zu α gehörigen Ansatz nicht gelöst werden, sobald m_2 eine Primzahl vom Typ 3) oder 5) enthält. — Auf diese Weise erhalten wir allenfalls unter den Vielfachen der Zahl m_1 eine Liste von „Kernzahlen".

5. Das Teilersymbol.

Wir nehmen jetzt aus $K(\sqrt[3]{2})$ zwei zueinander teilerfremde quadratfreie Zahlen $\alpha = (abc)$ und $\alpha' = (a'b'c')$ mit den ebenfalls zueinander teilerfremden quadratfreien Normen N und N'. Wir untersuchen die Frage, wann eine Zahl ohne Mittelglied $\Phi = (X\,0\,Y)$ gleich $\alpha\alpha'\varphi^2$ sein kann, und zwar im Zusammenhang mit den Möglichkeiten von $\Phi = \alpha\varphi^2$ und $\Phi = \alpha'\varphi^2$.

Das notwendige und hinreichende Kriterium für diese Ansätze besteht darin, daß die nach den Formeln (4) gebildeten Zahlen d_i bzw. d $(i = 1, 2, 3)$ quadratische Reste nach N bzw. N' sind. Nun ist

$$\alpha\alpha' = (abc)(a'b'c') = (aa' + 2bc' + 2cb' \;\; ab' + ba' + 2cc' \;\; ac' + ca' + bb')$$

und daher

$$\begin{aligned} d_2(\alpha\alpha') &= (ab' + ba' + 2cc')^2 - (aa' + 2bc' + 2cb')(ac' + ca' + bb') \\ &= d_1 d_2' + d_2 d_1' + \tfrac{1}{2} d_3 d_3'. \end{aligned}$$

Auf Grund von

$$d_2 : d_1 : d_3 = 1 : \sqrt[3]{4} : \sqrt[3]{16} \;(\alpha) \quad \text{bzw.} \quad d_2' : d_1' : d_3' = 1 : \sqrt[3]{4} : \sqrt[3]{16} \;(\alpha')$$

ergibt sich

$$d_2(\alpha\alpha') \equiv d_2 \cdot (d_1' \; \tfrac{1}{2} d_3' \; d_2') = d_2 \cdot \bar{\alpha}' \pmod{\alpha}$$

bzw.

$$d_2(\alpha\alpha') \equiv d_2' \cdot (d_1 \; \tfrac{1}{2} d_3 \; d_2) = d_2' \cdot \bar{\alpha} \pmod{\alpha'}$$

mit den konjugierten Werten $\bar{\alpha}$ und $\bar{\alpha}'$ zu α und α'. Beim Übergang von α zu einem Vielfachen $\alpha\alpha'$ multipliziert sich die maßgebende Zahl d_2 mit dem konjugierten Wert des hinzutretenden Faktors:

$$d_2(\alpha\alpha') \equiv d_2(\alpha) \cdot \bar{\alpha}' \pmod{\alpha} \tag{10}$$

und entsprechend verhält sich der quadratische Restcharakter mod N.

Wählen wir nun wieder α und α' (damit auch $\bar{\alpha}, \bar{\alpha}'$ sowie $\alpha\alpha'$) *primär*, so wird nach (6) für die maßgebenden Zahlen wenigstens das Jacobisymbol $+1$; also

$$\left(\frac{d_2}{N}\right) = \left(\frac{d_2'}{N'}\right) = \left(\frac{d_2(\alpha\alpha')}{NN'}\right) = +1, \text{ somit } \left(\frac{d_2(\alpha\alpha')}{N}\right) = \left(\frac{d_2(\alpha\alpha')}{N'}\right)$$

und daher nach Formel (10), die natürlich auch mit Vertauschung von α und α' gilt, immer

$$\left(\frac{\bar{\alpha}'}{\alpha}\right) = \left(\frac{\bar{\alpha}}{\alpha'}\right) \tag{11}$$

eine stets reziproke Beziehung.

Nehmen wir nun zwei natürliche Primzahlen p und q der Art $6n + 5$, so enthalten sie je einen primären Teiler 1. Grades (bis auf die irrelevante Multiplikation mit einem Einheitenquadrat). Setzen wir diese als α und α' in (11) ein, so läßt sich zwischen p und q eine eindeutige und stets symmetrische Relation definieren: Wir setzen

$$\left(\frac{\bar{\alpha}'}{\alpha}\right) = T(p/q)$$

und nennen dies das *Teilersymbol*. Es kann den Wert $+1$ oder -1 annehmen und stets gilt

$$T(p/q) = T(q/p),$$

wie immer sonst auch die beiden Primzahlen sein mögen (auch beide von der Form $4n + 3$).

Sollte jedoch eine Primzahl p der Art $6n + 1$ mit 2 als kubischem Rest vorliegen, so enthält sie drei solche primäre Teiler 1. Grades. Auch für diese läßt sich die analoge Relation aufstellen; bei Übertragung auf die natürliche Primzahl p aber erhalten wir 3 Teilersymbole, welche wohl zu unterscheiden sind, was wir etwa $(q = 6n + 5)$ durch

die Bezeichnung $T_1(p/q)$, $T_2(p/q)$, $T_3(p/q)$, kurz T_1, T_2, T_3 tun wollen. Auch hier gilt die Reziprozität und ferner ist

$$T_1 T_2 T_3 = +1,$$

weil hier $\bar{\alpha}_1 \bar{\alpha}_2 \bar{\alpha}_3 = p^2$ ist. Jeder der drei Idealteiler ist Träger eines T-Symbols.

Ist schließlich auch q von der Art $6n + 1$ mit 2 als kubischem Rest, so erhalten wir entsprechend neun T-Symbole $T_{ij}(p/q)$ $(i, j = 1, 2, 3)$. Wieder gilt die Symmetrie und auch

$$\prod_i T_{ij} = \prod_j T_{ij} = +1.$$

Der Wert eines jeden solchen T-Symbols läßt sich durch den quadratischen Restcharakter nach einer natürlichen Primzahl ermitteln, indem man eine rationale Kongruenzwurzel für $\sqrt[3]{2}$ einsetzt.

Für die Primzahl 3 wird stets $T = +1$; für Primzahlen mit 2 als kubischem Nichtrest sowie auch für 2 ist T zunächst nicht definiert. Wir wollen es aber in folgender Weise erweitern: Für erstere sei auch stets $T = +1$, für 2 sei T mit dem quadratischen Charakter der Einheit ε nach dem ungeraden Relationspartner erklärt. Besonders diese Erweiterung wird sich als wichtig erweisen. — $T(p/p)$ bleibe grundsätzlich nicht definiert.

Daraus ergeben sich alle Möglichkeiten für die Beziehungen zweier (verschiedener) Primzahlen zueinander:

Zwischen zwei Primzahlen der Art $3n + 2$ gibt es zwei Beziehungen: das (einzige) T-Symbol ist entweder $+1$ oder -1.

Zwischen einer Primzahl der Art $3n + 1$ (2 kubischer Rest) und einer der Art $3n + 2$ gibt es auch zwei Beziehungen: entweder alle drei T-Symbole $+1$ oder eines $+1$, die beiden andern -1.

Zwischen zwei Primzahlen der Art $3n + 1$ (2 kubischer Rest) gibt es drei Beziehungen: alle neun T-Symbole $+1$; fünf T-Symbole $+1$ (bei entsprechender Bezeichnung der „Rand", mit einem Index 1), die andern vier -1; nur drei Symbole $+1$ (bei entsprechender Bezeichnung die „Diagonale" T_{ii}), die sechs andern -1.

Wie wir sehen werden, spielen diese Beziehungen eine große Rolle bei unserem Problem.

Hiernach lassen sich auch T-Symbole für quadratfreie Oberzahlen (formale Zähler) nach der Regel $T(r/p) \cdot T(s/p) = T(rs/p)$ bilden. Solange dabei nur Primzahlen $3n + 2$ im Spiel sind, verbleibt das Symbol völlig eindeutig und gibt für $p = 6n + 5$ den quadratischen Restcharakter des Produktes der betreffenden konjugierten Zahlen 2. Grades nach dem Teiler 1. Grades von p an. — Sonst verdreifacht sich die Anzahl der Symbole mit jedem Primfaktor $3n + 1$ in entsprechender Weise.

Nach Kap. 4, Schluß zeigt das Teilersymbol an, ob eine Primzahl p beim Ansatz $(X\,0\,Y) = \alpha\varphi^2$ mit $N(\alpha) = m_1$ in m_2, dem quadratfreien Teil von X, auftreten kann. Dies ist für $p = 6n + 5$ möglich oder nicht, je nachdem $T = +1$ oder $T = -1$ ist. Das gilt auch für die Erweiterungen, besonders im Falle der Primzahl 2 nach Kap. 2, Schluß. Der Hinzunahme des Faktors 2 entspricht die Hinzunahme nichtprimärer Ansätze. — Für $p = 3n + 1$, 2 kubischer Rest, wird $p \mid m_2$ möglich oder nicht, je nachdem alle drei betreffenden T gleich $+1$ oder deren zwei gleich -1 sind. — Besteht m_1 selbst nur aus Primfaktoren $3n + 2$, so überträgt sich diese Entscheidung auf den gesamten Ansatz $X^3 + 4Y^3 = m_1 Z^2$ überhaupt (nur ein α).

Nunmehr kann man die Beziehung (10) auch mit $\alpha' = \beta$ und $N(\alpha) = p$ Primzahl in der Form schreiben

$$\left(\frac{d_2(\alpha\beta)}{N(\alpha)}\right) = \left(\frac{d_2(\alpha)}{N(\alpha)}\right) \cdot T(N(\beta)/N(\alpha)); \tag{12}$$

wieder völlig eindeutig, wenn alle beteiligten Primzahlen $\equiv 2(3)$ sind.

6. Aufbau von Unmöglichkeitskernzahlen.

Mit diesem Stande hätten wir nun das nötige Rüstzeug, um systematisch zum Aufbau von *Kernzahlen* zu schreiten. Beginnen wir mit dem einfachsten Falle, mit dem Produkte zweier Primzahlen p und q der Art $6n + 5$, deren primäre Teiler 1. Grades etwa α und β heißen mögen. Es sei also $m = m_1 m_2 = pqR$, wobei $R = \pm 1$ oder sonst nur Faktoren mit 2 als kubischem Nichtrest enthält. Ferner bedeute μ den quadratfreien Teil der Zahl $X + Y\sqrt[3]{4}$ (es ist $N(\mu) = m_1$). — Dann gibt es nach Ausscheidung des Falles $m_1 = 1$ sowie der nichtprimären Ansätze $\mu = \varepsilon\alpha$, $\mu = \varepsilon\beta$, $\mu = \varepsilon\alpha\beta$, welche nur bei geradem m möglich wären, folgende drei Möglichkeiten:

$$m_1 = p, \quad \mu = \alpha, \quad m_2 = qR;$$
$$m_1 = q, \quad \mu = \beta, \quad m_2 = pR;$$
$$m_1 = pq, \quad \mu = \alpha\beta, \quad m_2 = R.$$

In den ersten beiden Möglichkeiten müßte nach Kap. 4 der Faktor q bzw. p ein Teiler des betreffenden Polynoms sein, was unmöglich ist, wenn $T(p/q) = -1$ ist; die dritte Möglichkeit wird aber nach (6) und (12) für $T(p/q) = -1$ ebenfalls unmöglich. Somit ist pq *Kernzahl*, falls $T(p/q) = -1$ ist.

Das bedeutet, ausführlich ausgesprochen, den Satz:

Sind p und q zwei Primzahlen der Art $6n + 5$ mit $T(p/q) = -1$, so ist in jedem Körper $K(\sqrt{pqR})$, wo $R \gtrless 0$ höchstens Primzahlen der Art $3n + 1$ mit 2 als kubischem Nichtrest (oder noch 3) enthält, eine Gleichung $x^3 + y^3 = z^3$ unmöglich, und zwar auch bei durch 3 teilbarer Klassenzahl.

Beispiele mit durch 3 teilbarer Klassenzahl wären: $\sqrt{-1135}$ ($1135 = 5 \cdot 227$, $11^3 = 14^2 + 1135$), $\sqrt{-1927}$ ($1927 = 41 \cdot 47$, $4 \cdot 2^9 = 11^2 + 1927$).

Unsere Titelgleichung kann also nur in Fällen mit $T(p/q) = +1$ lösbar sein, wie es z. B. bei $\sqrt{85}$ geschieht, wo $T(5/17) = +1$ ist.

Als nächsten Schritt betrachten wir ein Produkt von mehreren Primzahlen der Art $6n + 5$. Der Einfachheit halber bezeichnen wir es selbst mit $m = m_1 m_2$, wobei sich dann dem Teil m_2 noch allfällig ein Faktor R aus lauter Primfaktoren mit 2 als kubischem Nichtrest anschließen kann. Wieder scheidet $m_1 = 1$ sowie jeder nichtprimäre Ansatz aus. In m_1 vereinigt sich also eine gewisse Teilmenge dieser Primzahlen (vielleicht auch alle), und μ mit $N(\mu) = m_1$ ist das Produkt der zugehörigen primären Primfaktoren 1. Grades aus $K(\sqrt[3]{2})$. Die restlichen Primzahlen aus m bilden dann m_2.

Nach den Ergebnissen im ersten Teil dieses Kapitels (Formel (12) und davor) muß nun einerseits für jeden Primteiler p_1 von m_1

$$T\left(\frac{m_1}{p_1}/p_1\right) = +1, \tag{13}$$

andrerseits auch für jeden Primteiler p_2 von m_2

$$T(m_1/p_2) = +1 \tag{14}$$

sein. Das heißt, die m_1 bildende (nicht leere) Teilmenge der Primzahlen von m muß so beschaffen sein, daß jede Primzahl aus m zu einer *geraden* Anzahl aus dieser Teilmenge in der Beziehung $T = -1$ steht. (Mag sie nun selbst dieser Teilmenge angehören oder nicht; innerhalb zählt sie selbst nicht mit — $T(p/p)$ ist nicht definiert —, sondern nur die anderen Faktoren von m_1; die 0 gilt als gerade Zahl.) Gibt es keine derartige Teilmenge, so ist m *Kernzahl*, d. h. es ist $x^3 + y^3 = z^3$ in jedem Körper $K(\sqrt{Rm})$ unmöglich, wo $R \gtrless 0$ keine weitere Primzahl mit 2 als kubischem Rest mehr enthält.

In dieses Schema fügt sich mit ihrem T-Symbol unter einer gewissen Umdeutung der Zahl m_1 auch die Primzahl 2 ein. Wir ordnen nämlich bei einem nichtprimären Ansatz $\mu = \varepsilon\alpha$, mit $N(\alpha) = m_1$ und α primär, 2 zur Teilmenge der (ungeraden) Faktoren von m_1, während wir beim primären Ansatz $\mu = \alpha$ die 2 außerhalb lassen (also in m_2). Für $\mu = \varepsilon$ bildet 2 allein die „innere Menge". Dann treffen nach der Definition von $T(2/N(\alpha)) = +1$ oder -1, je nachdem α in der Klasse ε^+ oder ε^- liegt, und nach Kapitel 2, Schluß, sowie Formel (7) die Regeln (13) und (14), wobei nun auch 2 in m_1 stehen kann, auch für diese Primzahl völlig zu und 2 spielt im Schema keine Ausnahmerolle mehr, wodurch wir nun im Gesamtbereich der Primzahlen $3n + 2$ operieren können und alle primären sowie nicht primären Ansätze erfassen. — Primzahlen $6n + 1$ (2 kubischer Rest) ziehen wir aber erst später in Betracht.

Dieses Schema läßt sich anschaulich darstellen durch einen *Graphen*. Wir zeichnen die Primzahlen von m (zunächst alle $\equiv 2(3)$) als Punkte und verbinden etwa zwei solche, die in der Beziehung $T = -1$ stehen, durch eine Linie. (Man könnte auch umgekehrt die mit $T = +1$ verbinden.) Für ein zu untersuchendes m sind die Punkte fest vorgegeben und ihr Graph kann auch isolierte Punkte enthalten (wenn für eine Primzahl stets $T = +1$ ist). Dann ist zur Lösbarkeit von $x^3 + y^3 = z^3$ in $K(\sqrt{m})$ oder $K(\sqrt{-m})$, allgemein $K(\sqrt{Rm})$ mit R wie oben, notwendig, daß der zu m gehörige Graph irgendeine Teilmenge von Punkten enthält, zu welcher von jedem Punkte — innerhalb oder außerhalb von ihr gelegen — eine *gerade* Anzahl von Linien führt. Diese Teilmenge muß also unter sich einen Eulerschen Graphen bilden und außerdem aber noch bezüglich jenes äußeren Punktes in „gerader Lage" sein. Diese „Innenpunkte" bilden das m_1, die „Außenpunkte" das m_2. Wir wollen eine solche Teilmenge eine *lösende Teilmenge*, kurz eine *Lösung* nennen. In Fig. 1 und Fig. 2 bilden die eingekreisten Punkte eine solche Lösung.

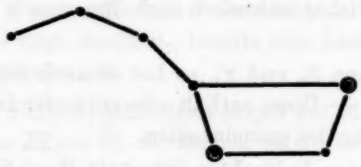

Fig. 1

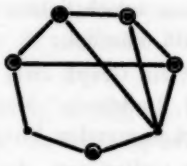

Fig. 2

Ein isolierter Punkt bildet stets eine brauchbare Lösung, nicht jedoch die leere Menge; ferner ist die Gesamtmenge als Lösung zugelassen.

Hingegen besitzt, wie einfache Beispiele zeigen, nicht jeder Graph eine lösende Teilmenge; so z. B. nicht folgende Graphen mit 4 Punkten:

Fig. 3

Fig. 4

Fig. 5

Jeder Graph ohne Lösung liefert eine Kernzahl. Einen Graphen von Fig. 3, 4, 5 bilden die Primzahlen 2, 11, 41, 71 bzw. 5, 11, 17, 23 bzw. 2, 5, 17, 23. Daher sind Kernzahlen $2 \cdot 11 \cdot 41 \cdot 71 = 64042$, $2 \cdot 5 \cdot 17 \cdot 23 = 3910$, $5 \cdot 11 \cdot 17 \cdot 23 = 21505$ (s. Tabelle am Schluß).

Dazu liefert $\sqrt{-13 \cdot 3910}$ ein Beispiel mit durch 3 teilbarer Klassenzahl (ersichtlich aus $29^3 = 2 \cdot 5 \cdot 17 + 13 \cdot 23 \cdot 9^2$).

Auch ein Graph mit einer beliebigen *geraden* Anzahl von Punkten, welche nur getrennt paarweise verbunden sind (regulärer Graph 1. Grades), oder wo alle Verbindungslinien gezogen sind (vollständiger Graph), hat keine Lösung. — Es gibt also Kernzahlen von beliebig hoher Zusammensetzung.

Daß jeder Graph auch an (unendlich vielen) Primzahlkombinationen verwirklicht wird, ergibt sich aus dem Satz, daß in jeder Restklasse eines beliebigen Moduls (zu diesem teilerfremd) stets unendlich viele Primideale 1. Grades vorhanden sind.

Hingegen besitzt ein Graph mit *ungerader* Punktezahl immer eine Lösung, welcher Satz nun in einem eigenen Einschubkapitel gezeigt sei.

7. Ein Satz über Graphen.

Wir wollen also folgenden Satz beweisen:

In jedem (endlichen) Graphen mit ungerader Punkteanzahl gibt es eine (nicht leere) Teilmenge von Punkten, zu der von jedem Punkte eine gerade Anzahl von Linien führt.

Wir betrachten hier naturgemäß nur Graphen ohne Zweiecke, wo also zwischen zwei Punkten höchstens eine Linie gezogen ist. Übrigens überträgt sich der Satz sofort auch auf Graphen mit Zweiecken, da ja die Linienzahl nur mod. 2 genommen wird. Mit sich selbst ist kein Punkt verbunden zu denken, also ohne „Schlingen". — Man kann dem Satz auch folgende textliche Einkleidung geben: Unter einer ungeraden Anzahl von Personen findet sich immer ein Kreis, so daß jede Person eine gerade Anzahl aus diesem Kreise kennt (kennen dabei als symmetrische, nicht reflexive Relation verstanden).

Da der Satz für die Punktezahl 1 trivial und auch für die Anzahl 3 leicht nachgeprüft ist, verwenden wir den Schluß von n auf $n + 2$. Zunächst schicken wir noch einen aus der Definition der lösenden Teilmenge (die im Satz genannte Eigenschaft) unmittelbar ersichtlichen *Hilfssatz* voraus, welcher nebenbei auch für gerade Punkteanzahl gilt, nämlich:

Hat ein Graph zwei verschiedene Lösungen $\mathfrak{L}_1$ und $\mathfrak{L}_2$, so hat er auch eine dritte: die „mod. 2 addierte" Menge $\mathfrak{L}_1 + \mathfrak{L}_2 - \mathfrak{L}_1\mathfrak{L}_2$. — Diese enthält alle entweder in $\mathfrak{L}_1$ oder in $\mathfrak{L}_2$ vorkommenden Punkte, unter Weglassung der gemeinsamen.

Wir wollen nun, da kein Mißverständnis zu befürchten ist, statt $\mathfrak{L}_1 + \mathfrak{L}_2 - \mathfrak{L}_1\mathfrak{L}_2$ einfach $\mathfrak{L}_1 + \mathfrak{L}_2$ schreiben, also für die Addition mod. 2 das Operationszeichen $+$ benützen[2]).

Denn allgemein addieren sich für irgend zwei Teilmengen $\mathfrak{M}_1$ und $\mathfrak{M}_2$ die Anzahlen der zu einem Punkte P führenden Linien mod 2; sind diese Linienzahlen s_1, s_2, s_3 für $\mathfrak{M}_1, \mathfrak{M}_2$ und $\mathfrak{M}_3 = \mathfrak{M}_1 + \mathfrak{M}_2$, so ist $s_3 \equiv s_1 + s_2 (2)$. Für lösende Teilmengen sind dann alle diese Zahlen für jeden Punkt P gerade.

Danach ergeben sich aus k unabhängigen Lösungen im Ganzen $2^k - 1$ Lösungen, nämlich alle solchen „Linearkombinationen". Sie bilden nach $\mathfrak{L} + \mathfrak{L} = 0$ zusammen mit der Nullmenge als Einheitselement eine Abelsche Gruppe vom Typ 2, 2, . . ., 2.

---

[2]) Diese Summendefinition findet sich auch bei *O. Veblen*, Analysis Situs (New York, 2. Aufl. 1931, S. 10).

Nunmehr greifen wir irgendeinen Punkt P heraus; er sei insgesamt mit r Punkten $A_1, A_2, \ldots, A_r$ verbunden. (Ein isolierter Punkt bietet sofort eine Lösung.) Die r Graphen, welche durch Weglassen von P und A_1, von P und $A_2, \ldots$, von P und A_r entstehen, also je um 2 Punkte weniger enthalten, haben laut Induktionsvoraussetzung ihrerseits lösende Teilmengen, welche $\mathfrak{L}_1, \mathfrak{L}_2, \ldots, \mathfrak{L}_r$ heißen mögen. Diese Mengen brauchen nicht alle verschieden zu sein; sie können teilweise oder ganz zusammenfallen. Von jedem der außer P und den A_i noch übrigen Punkten (falls solche noch vorhanden) führt zu jeder $\mathfrak{L}_i$ und daher auch zu jeder Kombination aus ihnen eine gerade Anzahl von Linien, ebenso von A_i zu $\mathfrak{L}_j$ für $i \neq j$; fraglich ist nur die betreffende Lage von A_i zu $\mathfrak{L}_i$ sowie von P zu allen $\mathfrak{L}$.

Wir zählen nun die verschiedenen $\mathfrak{L}_i$, zu denen A_i gerade liegt. Da sind die drei Fälle denkbar:

1) Mindestens zwei der A_i (etwa A_1 und A_2) liegen zu $\mathfrak{L}_i$ gerade, wobei auch $\mathfrak{L}_1 \neq \mathfrak{L}_2$ ist.

2) Mindestens ein A_i (etwa A_1) liegt zu A_i gerade; aber (falls überhaupt mehrfach) alle diese $\mathfrak{L}_i$ sind gleich $\mathfrak{L}_1$.

3) Kein A_i liegt zu $\mathfrak{L}_i$ gerade.

Im Falle 1) bilden $\mathfrak{L}_1$ und $\mathfrak{L}_2$, daher auch $\mathfrak{L}_1 + \mathfrak{L}_2$ eine Lösung für das System ohne P (mit gerader Punktezahl). Zu einer dieser drei Mengen liegt aber sicher P gerade, welche damit auch eine Lösung des Gesamtsystems vorstellt.

Im Falle 2) stellt $\mathfrak{L}_1$ eine Lösung für das System ohne P dar. Es liege etwa für $i = 1, 2, \ldots, k$ der Punkt A_i zu $\mathfrak{L}_i = \mathfrak{L}_1$ gerade, für $i = k + 1, \ldots, r$ aber A_i zu $\mathfrak{L}_i$ ungerade. (Eventuell auch nur $k = 1$.) Dann liegen zur Menge $\mathfrak{L}_{k+1} + \cdots + \mathfrak{L}_r = \mathfrak{R}$ alle Punkte $A_{k+1}, \ldots, A_r$ ungerade. Sämtliche noch übrigen Punkte (außer P) aber liegen zu $\mathfrak{R}$ gerade. Im Teilgraphen, den diese Menge bildet, sind also die $A_{k+1}, \ldots, A_r$, soweit sie ihr selbst angehören, Knotenpunkte ungeraden Grades. Jeder Graph enthält aber Knotenpunkte ungeraden Grades in einer geraden Anzahl. Die Menge $\mathfrak{R}$ enthält also eine gerade Anzahl dieser Punkte. Ganz das Gleiche findet man aber auch für die Menge $\mathfrak{L}_1 + \mathfrak{R}$. Daher muß auch die „Summe" dieser beiden Mengen, das ist $\mathfrak{L}_1$, eine gerade Anzahl aus $A_{k+1}, \ldots, A_r$ enthalten, und, da $\mathfrak{L}_1 = \mathfrak{L}_2 \cdots = \mathfrak{L}_k$ die Punkte $A_1, A_2, \ldots, A_k$ per definitionem nicht enthält, eine gerade Anzahl von A-Punkten überhaupt. Nachdem aber die A genau die mit P verbundenen Punkte sind, bedeutet das soviel wie, daß P zu $\mathfrak{L}_1$ gerade liegt, somit $\mathfrak{L}_1$, bereits eine Lösung das System ohne P, auch eine Lösung das Gesamtsystems ist.

Im Falle 3) schließlich liegen zur Menge $\mathfrak{L}_1 + \mathfrak{L}_2 + \cdots + \mathfrak{L}_r = \Sigma\mathfrak{L}_i$ alle A_i ungerade (also $\Sigma\mathfrak{L}_i \neq 0$). Sie stellen, sofern sie ihr selbst angehören, die Knotenpunkte ungeraden Grades dar, sind also in gerader Anzahl in ihr vorhanden. Das heißt, P liegt zu $\Sigma\mathfrak{L}_i$ gerade. *Füge ich nun P zu $\Sigma\mathfrak{L}_i$ dazu*, so geht die ungerade Lage aller A in die gerade über, während sich die gerade Lage der sonstigen, mit P nicht verbundenen Punkte nicht ändert. Ich komme also auch hier zu einer, sogar mindestens zwei Punkte enthaltenden, Gesamtlösung in der Gestalt $\Sigma\mathfrak{L}_i + P$.

Damit ist der Satz vollends bewiesen.

8. Weiteres über Kernzahlen und Ausblick.

Für unser Problem bedeutet dieser Graphensatz zunächst, daß eine Zahl der Art $3n + 2$, die aus lauter Primfaktoren dieser Art besteht, nicht Kernzahl ist.

Um nun auch die Primzahlen $3n + 1$ (2 kubischer Rest) einzubeziehen, bedenken wir, daß ein solches p bezüglich jedes Ansatzes zwei unabhängige T-Symbole hat und ihr Produkt als drittes; und ferner, daß p genau dann Teiler des Polynomes mit dem quadratfreien Teil m_2 ist, wenn alle drei, also alle zwei unabhängigen T-Symbole $+ 1$ sind. Demnach wird im Graphen eine Primzahl der Art $3n + 1$ durch *zwei* Punkte vertreten. Dabei besteht für diese Punkte eine gewisse Freiheit, nämlich eine Auswahl aus drei „Vorlagen", welche bezüglich jedes anderen Punktes durch eine gerade Summe der entsandten Linien (also 000, 011, 101, 110) untereinander gebunden sind. Daraus resultieren drei Graphen. Außerdem ist es grundsätzlich gleichgültig, ob man sich die beiden p-Punkte verbunden denkt oder nicht, so daß die Zahl auf 6 Möglichkeiten steigt. Bei Hinzunahme von k Primzahlen der Art $3n + 1$ (2 kubischer Rest) steigt die Zahl auf 6^k Graphen, welche aber nicht alle verschieden (oder gar topologisch wesentlich verschieden) zu sein brauchen.

Gibt es bei all diesen möglichen Graphen keine „lösende Teilmenge", so liegt eine Kernzahl vor. Das ist z. B. der Fall bei Fig. 3 (Kap. 6), wenn etwa die oberen Punkte mit p, die unteren mit q und r, zwei Primzahlen der Art $3n + 2$, besetzt werden. Die 5 anderen zugehörigen Graphen gleichen dann topologisch Fig. 4 oder Fig. 5, womit in keinem Falle eine Lösung existiert.

Dieser Typ ist etwa für $p = 31$, $q = 2$, $r = 41$ realisiert. Also ist $2 \cdot 31 \cdot 41 = 2542$ eine Kernzahl. Es gibt also auch Kernzahlen mit einem Primfaktor der Art $3n + 1$.

Besitzt andrerseits ein Graph mit zweifachen p-Punkten (gleichgültig ob mit ungerader oder gerader Gesamtpunktezahl) eine lösende Teilmenge, so ist sie, falls sie beide Punkte einer Primzahl enthält, zunächst zwar unbrauchbar, kann aber immer in eine Lösung verwandelt werden, welche nur einen p-Punkt enthält. Dazu braucht man nur einen p-Punkt aus $\mathfrak{L}$ herauszunehmen und seine Verbindungslinien auf den anderen p-Punkt zu übertragen; allfällig entstehende Doppellinien sind zu streichen, also mod 2 zu übertragen. Dann ist dieser in $\mathfrak{L}$ verbleibende p-Punkt durch den dritten an sich möglichen ersetzt, was einen erlaubten Operator, den Übergang zu einem gleichberechtigten Graphen, darstellt. Und alles bleibt in gerader Lage, also der Lösungscharakter erhalten. Auf diesem Wege kann man schrittweise alle „Doppelpunkte" aus der Lösung entfernen, und wir kommen zu einer unmittelbar brauchbaren Lösung, welche von jeder Primzahl $\equiv 1\ (3)$ höchstens noch einen Punkt enthält.

Da nun eine beliebige Zahl der Art $3n + 2$ stets einer ungeraden Punkteanzahl entspricht und bei einer solchen für jeden Graphen eine Lösung existiert, haben wir somit den allgemein gültigen Satz:

Es gibt keine Unmöglichkeitskernzahl der Art $3n + 2$.

Dieses Ergebnis scheint — zumal hier auch die Klassenzahl kein Hindernis ist — darauf hinzudeuten, daß $x^3 + y^3 = z^3$ in $K(\sqrt{m})$ für $|m| \equiv 2(3)$ stets lösbar ist, was ich hiermit als Vermutung aussprechen möchte. Tatsächlich ist auch, soweit ich sehe, noch in keinem solchen Falle ein Unmöglichkeitsbeweis geführt, während zahlreiche Beispiele für die Lösbarkeit vorhanden sind. Freilich ist dies damit noch lange nicht bewiesen. Es gibt ja auch im Falle $|m| \equiv 1\ (3)$ Zahlen, die in unserm Sinne keine Kernzahlen sind, und wo doch die Unmöglichkeit gilt — schon auf Grund einer nicht durch 3 teilbaren Klassenzahl. Und da bleibt wieder die Frage offen, ob vielleicht etwa für Zahlen, die nicht auf einer Kernkette liegen, und bei durch 3 teilbarer Klassenzahl die Gleichung immer möglich ist.

Zum Abschluß gebe ich eine Tabelle der T-Symbole für die Primzahlen unter 100:

	2	5	11	17	23	29	31_1	31_2	41	43_1	43_2	47	53	59	71	83	89
2		−	−	−	−	+	+	−	+	+	−	−	+	−	+	+	−
5	−		−	+	−	−	−	−	−	−	+	+	−	+	−	−	+
11	−	−		−	+	−	−	+	+	+	+	−	−	−	+	+	−
17	−	+	−		+	−	−	−	+	−	+	−	+	−	+	−	−
23	−	−	+	+		+	+	−	−	+	−	−	+	+	−	−	+
29	+	−	−	−	+		+	+	−	−	+	+	−	−	−	−	−
31_1	+	−	−	−	+	+			−	+	+	−	−	+	+	−	−
31_2	−	−	+	−	−	+			+	−	+	+	−	+	+	−	+
41	+	−	+	+	−	−	−	+		−	−	−	+	−	−	+	−
43_1	+	−	+	−	+	−	+	−	−			+	+	−	−	+	−
43_2	−	+	+	+	−	+	+	+	−			+	−	−	+	+	+
47	−	+	−	−	−	+	−	+	−	+	+		+	−	−	+	−
53	+	−	−	+	+	−	−	−	+	+	−	+		+	−	+	−
59	−	+	−	−	+	−	+	+	−	−	−	−	+		−	+	+
71	+	−	+	+	−	−	+	+	−	−	+	−	−	−		−	+
83	+	−	+	−	−	−	−	−	+	+	+	+	+	+	−		−
89	−	+	−	−	+	−	−	+	−	−	+	−	−	+	+	−	

Sie dient zum Aufsuchen oder Ablesen von Unmöglichkeits-Kernzahlen; eine solche ist z. B. $2 \cdot 5 \cdot 17 \cdot 47 \cdot 53 \cdot 59$, weil der Graph dieser Primzahlen keine Lösung hat.

Eingegangen 20. Januar 1954.

Einige Sätze über Lagebeziehungen in endlichen Graphen.

Von *Alexander Aigner* in Graz.

Anläßlich eines zahlentheoretischen Problems[1]) hatte ich den dort benötigten Satz bewiesen:

Satz 1. *In jedem endlichen Graphen mit einer ungeraden Anzahl von Punkten gibt es eine (nicht leere) Teilmenge, zu der von jedem Punkt aus eine gerade Anzahl von Linien führt (Geradlösung, kurz Lösung genannt).*

Nunmehr möchte ich etwas näher auf dieses Gebiet, das auch in einer etwas anderen Richtung liegt als sonstige Untersuchungen über Graphen, eingehen und einige ähnliche Sätze bringen.

Zunächst einige vorbereitende Klarstellungen. Für uns ist der Graph eine beliebige Auswahl von Linien zwischen fest vorgegebenen Punkten, kann also — im Gegensatz zur meist üblichen Auffassung — auch isolierte Punkte enthalten. Dadurch unterscheiden sich auch (trotz einiger Verwandtschaft) die Geradlösungen etwa von den Eulerschen Teilgraphen. Auch ist umgekehrt nicht jeder Eulersche Teilgraph eine Geradlösung, weil hierbei auch die Stellung der Punkte außerhalb des Teilgraphen mitspielt. — Da es sich im wesentlichen um Linienzahlen mod. 2 handelt, genügt es, nur Graphen ohne Doppellinien zu betrachten, bei denen also zwischen zwei Punkten nur eine oder keine Linie führt. Ferner sei kein Punkt mit sich selbst verbunden (Graphen im engeren Sinne).

Wenn nun, wie in Satz 1, die Linien von einem Punkte P zu einer Teilmenge $\mathfrak{M}$ (die auch die Gesamtmenge sein kann) gezählt werden, so zählen hierbei, falls P der Teilmenge $\mathfrak{M}$ selbst angehört, nur die anderen Punkte von $\mathfrak{M}$; falls P außerhalb von $\mathfrak{M}$ liegt, zählen alle Punkte von $\mathfrak{M}$. Ist diese Zahl gerade bzw. ungerade, so wollen wir kurz sagen: *P liegt zu $\mathfrak{M}$ gerade bzw. ungerade.*

Danach können wir auch die Lage zweier beliebiger Teilmengen (des vorgegebenen Systems von endlich vielen Punkten) zueinander als gerade oder ungerade definieren, mögen diese Mengen nun zueinander fremd sein oder nicht, indem wir die zu einer Menge von den Punkten der anderen Menge ausgehenden Linienzahlen über alle diese Punkte summieren. (Die Linien zwischen den gemeinsamen Punkten werden dabei doppelt gezählt.) Daraus ergibt sich, weil bei Vertauschung der beiden Mengen genau dieselbe Zahl resultiert, eine stets symmetrische Beziehung. Zu sich selbst liegt jede Menge gerade, weil hier alle Linien doppelt zu zählen sind. Eine *Lösung* liegt dann nicht nur zu jedem Punkt, sondern zu jeder beliebigen Menge gerade. — Ein isolierter Punkt ist stets eine Lösung.

Unter der *Summe* zweier Mengen $\mathfrak{M}_1 + \mathfrak{M}_2$ soll hier die Menge verstanden werden, welche alle Punkte enthält, die einer und nur einer der beiden Mengen angehören. Dann

[1]) *A. Aigner*, Die kubische Formatgleichung in quadratischen Körpern, Journ. f. r. u. a. Math. **195** (1955), 3—17.

ist stets $\mathfrak{M} + \mathfrak{M} = 0$. Die Summe mehrerer Mengen enthält dann genau die Punkte, die in einer ungeraden Anzahl dieser Mengen vorkommen. (Für fremde Mengen läuft das auf die gewöhnliche Summe hinaus.)

Setzen wir ein Vorzeichen $\operatorname{sig}(\mathfrak{M}, \mathfrak{N}) = +1$ für gerade, -1 für ungerade Lage, so gilt allgemein

$$\operatorname{sig}(\mathfrak{M}_1 + \mathfrak{M}_2, \mathfrak{N}) = \operatorname{sig}(\mathfrak{M}_1, \mathfrak{N}) \cdot \operatorname{sig}(\mathfrak{M}_2, \mathfrak{N}),$$

d. h. eine Menge (die auch ein Einzelpunkt sein kann) liegt zur Summe gerade, wenn sie zu beiden Summanden gleichartig liegt. Entsprechend entscheidet bei mehr Summanden die Anzahl der ungerade liegenden.

Die Gesamtheit der Lösungen eines Graphen bildet zusammen mit der leeren Menge bezüglich dieser Summenbildung eine Abelsche Gruppe vom Typ $2, 2, 2, \ldots, 2$. Bei k unabhängigen gibt es insgesamt $2^k - 1$ Lösungen. — Die Gesamtheit aller Teilmengen bildet bei n Punkten eine solche Gruppe der Ordnung 2^n. Alle zu einer Menge, die keine Lösung ist, gerade liegenden Teilmengen bilden darin eine Untergruppe vom Index 2.

Wir führen nun den Begriff *Bild* (Ungeradheitsbild) einer solchen Punktmenge $B(\mathfrak{M})$ ein und verstehen darunter die Gesamtheit aller Punkte des Graphen, die zu $\mathfrak{M}$ ungerade liegen.

Für eine Lösung wird $B = 0$; es ist auch stets $B(0) = 0$. Ferner gilt, wie man leicht sieht, das Gesetz $B(\mathfrak{M} + \mathfrak{N}) = B(\mathfrak{M}) + B(\mathfrak{N})$.

Die Gesamtheit der Bilder bildet daher auch eine Gruppe, und zwar eine Untergruppe der Teilmengengruppe vom Index 2^k, wenn es k unabhängige Lösungen gibt. (Sie entspricht der Faktorgruppe nach der Lösungengruppe.) Für $k = 0$ besteht einstufige Isomorphie; jede Menge ist ein Bild.

Man sieht sogleich: Ein Bild kann Punkte, die einer und derselben Lösung $\mathfrak{L}$ angehören, nur paarweise, in gerader Anzahl, enthalten. (Denn eine Lösung liegt ja zu einer beliebigen Teilmenge gerade.) Und auch die Umkehrung: Eine Teilmenge, deren Punkte in allen Bildern nur paarweise auftreten, ist eine Lösung. Demnach sind unter den Teilmengen die Bilder durch die notwendige und hinreichende Bedingung gekennzeichnet, daß aus jeder Lösung nur eine gerade Anzahl von Punkten vorkommt. Die Punkte aber, die keiner Lösung angehören (falls solche vorhanden), sind frei kombinierbar; sie können in jeder beliebigen Zusammenstellung auftreten. Im besonderen allein, d. h. es gibt eine Menge, zu der nur dieser eine Punkt ungerade liegt.

Aus dieser Struktur der Bildermenge ergeben sich dann verhältnismäßig rasch die folgenden Sätze.

Satz 2. *Hat ein Graph mit gerader Punktezahl eine Geradlösung, so hat er auch eine zweite unabhängige, d. h. mindestens drei Lösungen.*

Beweis. Es sei $\mathfrak{L}$ eine solche Lösung. Entferne ich nun einen $\mathfrak{L}$ angehörigen Punkt P aus dem Graphen, so hat das verbleibende Teilsystem mit ungerader Punktezahl nach Satz 1 für sich eine Lösung $\mathfrak{L}_1$. Zu dieser Menge liegen also alle Punkte außer P sicher gerade. Da aber das Bild von $\mathfrak{L}_1$ im Gesamtgraphen nicht aus P allein bestehen kann (P ist Angehöriger der Lösung $\mathfrak{L}$, die in jedem Bilde paarweise auftreten müssen!), so muß auch P zu $\mathfrak{L}_1$ gerade liegen, welche somit eine zweite, und zwar sicher von $\mathfrak{L}$ verschiedene Lösung darstellt ($\mathfrak{L}$ enthält P, $\mathfrak{L}_1$ nicht).

Nach demselben Verfahren lassen sich die Sätze 1 und 2 zusammenfassend weitgehend verallgemeinern:

Satz 3. *Ein Graph mit ungerader Punktezahl hat eine ungerade, ein Graph mit gerader Punktezahl eine gerade Anzahl unabhängiger Lösungen* (einschließlich 0).

Beweis. Angenommen, der Satz gelte schon bis zu einer gewissen Höhe, so daß bei ungerader Punktezahl aus $2k - 2$ unabhängigen Lösungen, bei gerader Punktezahl aus $2k - 1$ solchen immer eine weitere folgt; wie es bereits geschieht für $k = 1$.

Es gebe nun bei ungerader Punktezahl $2k$ unabhängige Lösungen. Diese kann man aus allen $2^{2k} - 1$ Lösungen stets so auswählen, daß ein bestimmter Punkt P, welcher überhaupt darin erscheint, nur in einer einzigen Lösung vorkommt, in den anderen $2k - 1$ Lösungen nicht. Diese $2k - 1$ Lösungen sind nun auch Lösungen des Systems ohne P (mit gerader Punktezahl), in welchem es aber dann laut Voraussetzung eine neue unabhängige Lösung gibt. Diese neue ist aber auch Lösung des Gesamtsystems, weil nicht P allein zu ihr ungerade liegen kann. Und die erste alte Lösung, die ja noch da ist, kann auch durch den Einschluß der neuen nicht abhängig werden, weil sie ja als einzige den Punkt P enthält. Somit haben wir insgesamt $2k + 1$ unabhängige Lösungen gewonnen.

Nunmehr nehmen wir bei gerader Punktezahl $2k + 1$ unabhängige Lösungen an. Wieder können sie so ausgewählt werden, daß ein Punkt P nur in einer vorkommt. Die $2k$ übrigen sind auch Lösungen des Systems ohne P, welches nach dem soeben Bewiesenen noch eine neue solche hat, die sich wie vorhin auch als Lösung des Gesamtsystems erweist. Ihr Hinzukommen hebt die Unabhängigkeit der ersten alten Lösung, die P enthält, nicht auf und somit hat sich die Anzahl auf $2k + 2$ erhöht. — Damit ist für beide Teile des Satzes der Schritt von k auf $k + 1$ getan.

Es sind also bei ungerader Punktezahl insgesamt 1, 7, 31, . . ., bei gerader Punktezahl 0, 3, 15, . . . Lösungen möglich; diese Typen existieren auch wirklich alle, wie triviale Beispiele mit isolierten Punkten sogleich zeigen. Der relativ große Unterschied der Lösungszahlen erleichtert auch die praktische Entscheidung in einem vorgelegten Beispiel.

Ferner gilt das auch als Konstruktionsprinzip brauchbare Übergangsgesetz:

Satz 4. *Durch Anfügen oder Weglassen eines Punktes entsteht immer ein Nachbartyp.* Also z. B. aus Typ 1 der Typ 0 oder 3, aus Typ 15 der Typ 7 oder 31. — Der Typ 0 geht dabei stets in den Typ 1 über.

Beweis. Aus gruppentheoretischen Gründen kommt ein irgendwie neu eingefügter Punkt immer entweder zu allen Lösungen des alten Systems oder zur Hälfte von ihnen (einschließlich der Nullmenge gerechnet) gerade zu liegen. Ebenso befindet sich ein wegzulassender Punkt stets entweder außerhalb jeder oder außerhalb jeder zweiten Lösung. Es bleiben also in den erstgenannten Fällen alle, in den zweitgenannten die Hälfte der Lösungen bestehen; daher werden sowohl beim Anfügen als auch beim Weglassen mindestens die Hälfte der Lösungen erhalten.

Dabei tritt in den Fällen, wo alle alten Lösungen bleiben, nach Satz 3 sogar Vermehrung ein; in den anderen Fällen — aus dem inversen Vorgang zu schließen — auch wirklich Verminderung. Entweder hat das (um einen Punkt) größere oder das kleinere System die höhere (mit der Nullmenge die doppelte) Lösungszahl. Es gibt also die zwei direkt oder invers ausführbaren Vorgänge: Der neue Punkt beläßt alle Lösungen und schafft noch ebensoviel neue, denen er angehört; — oder er zerstört die Hälfte der Lösungen und schafft auch keine neuen (denen er angehören würde).

Daraus ergibt sich, als Zusammensetzung von zwei solchen Schritten, unmittelbar:

Satz 5. *Bei Zufügen oder Weglassen (Umänderung) einer Linie entsteht immer derselbe oder ein zweitnächster Typ.*

Dasselbe gilt auch bei Umänderung mehrerer von einem Punkte ausgehender Linien.

Wir betrachten schließlich „*Ungeradlösungen*" $\mathfrak{U}$, das sind Mengen, zu denen jeder Punkt des Graphen ungerade liegt. Sie sind *Urbilder* der Gesamtmenge. Über ihre Möglichkeit ergibt sich sofort:

Satz 6. ***Es existiert dann und nur dann eine Ungeradlösung, wenn es keine Geradlösung mit ungerader Punktezahl gibt.***

Sei es, daß es überhaupt keine Geradlösung oder nur solche mit gerader Punktezahl gibt.

Beweis. Für jede Geradlösung $\mathfrak{L}$ mit gerader Punktezahl erfüllt offenbar die Gesamtmenge die Bedingung, eine gerade Anzahl von Punkten aus $\mathfrak{L}$ zu enthalten, für eine $\mathfrak{L}$ mit ungerader Punktezahl aber nicht. Nur bei Fehlen von letzteren ist die Gesamtmenge ein Bild.

Für eine beliebige Menge $\mathfrak{M}$ wird sig $(\mathfrak{M}, \mathfrak{U}) = (-1)^m$, wo m die Punktezahl von $\mathfrak{M}$ bedeutet. $\mathfrak{U}$ liegt also zu Mengen mit gerader Punktezahl gerade, zu Mengen mit ungerader Punktezahl ungerade. Schon das würde sich mit einer $\mathfrak{L}$ von ungerader Punktezahl nicht vertragen. Da ferner $\mathfrak{U}$ wie jede Menge zu sich selbst gerade liegt, so muß jede $\mathfrak{U}$ eine gerade Punktezahl haben. (Das geht auch schon daraus hervor, daß sie einen Teilgraphen mit lauter Knotenpunkten ungeraden Grades bildet.)

Geradlösungen $\mathfrak{L}$ und Ungeradlösungen $\mathfrak{U}$ bilden nach den schematischen Regeln

$$\mathfrak{L} + \mathfrak{L} = \mathfrak{L}, \mathfrak{L} + \mathfrak{U} = \mathfrak{U}, \mathfrak{U} + \mathfrak{U} = \mathfrak{L}$$

zusammen eine Gruppe, gegenüber der $\mathfrak{L}$-Gruppe (einschließlich 0) auf den doppelten Umfang erweitert; die $\mathfrak{U}$ sind daher, sofern überhaupt, in Anzahl einer Zweierpotenz vorhanden, um 1 mehr als die eigentlichen $\mathfrak{L}$. Bemerkenswert ist noch, daß die $(\mathfrak{L} - \mathfrak{U})$-Gruppe nie aus der Null allein besteht.

Gibt es keine Geradlösung — was nach Satz 1 nur bei gerader Punktezahl des Gesamtsystems möglich ist —, so entfällt jede einschränkende Bedingung für die Bilder. Jede Teilmenge ist ein Bild. Die Zuordnung von Bild und Urbild ist ein-eindeutig, auch ein bezüglich der Addition richtiggehender Automorphismus. Es gibt dann auch nur eine einzige Ungeradlösung, das Urbild der Gesamtmenge. Unter Umständen (wenn der Graph nur Knotenpunkte ungeraden Grades aufweist) ist es dieser selbst gleich.

Eingegangen 20. Januar 1954.

La paraanalitikaj funkcioj en n dimensioj.

De *Maurice Fréchet* en Paris.

Résumé.

L'auteur développe ici deux des notes qu'il a présentées en 1953 aux Comptes-Rendus, notes (citées plus loin) où il donnait la définition des fonctions paraanalytiques et indiquait des propriétés de ces fonctions qui généralisent des propriétés importantes des fonctions analytiques classiques.

Le texte qui suit a été écrit dans la langue internationale Esperanto, comme celui de deux mémoires sur le même sujet parus dans les Annali di Matematica et dans Compositio Mathematica et cités plus loin.

Rememorigo. Monogenaj (aŭ deriveblaj) funkcioj. Estu $F(z) = P(x, y) + iQ(x, y)$ kompleksa funkcio de la kompleksa varianto $z = x + iy$. Oni diras, ke ĝi estas *monogena* en la punkto $z^0 = x^0 + iy^0$, se la kvociento $\frac{\Delta F}{\Delta z}$ konverĝas, kiam $\Delta z \to 0$, al unika limo F'_0, kiun oni nomas la derivaĵo de $F(z)$ por $z = z^0$. Pro tio ni preferas diri, ke la funkcio estas *derivebla* en la punkto z^0.

Tia difino ne estas konvena por la ĝeneraligo al kiu ni celas. Sed ni pruvis antaŭe (Fréchet, [2])[1]) ion, kio cetere estas facile pruvebla, nome, ke tiu difino estas *ekvivalenta* al la jena difino:

La funkcio $F(z)$ estas *derivebla* (aŭ *monogena*) en la punkto z^0 se

1° *ĝi estas diferencialebla en tiu punkto*[2]),

2° *la kvociento* $\left(\frac{dF}{dz}\right)_{z=z^0}$ *estas sendependa de dz.* (Tiu kvociento egalas la derivaĵon F'_0.)

Alivorte ekzistas kompleksa nombro $F'_0 = A + iB$ tiel, ke oni havas

$$(dP)_{z=z^0} + i(dQ)_{z=z^0} = (A + iB)(dx + idy) \tag{1}$$

Tiu egalaĵo, en kiu ĉio estas reala krom la simbolo i, *ekhavas sencon nur post adopto de la bone konata regulo de multiplikado*:

$$1 \cdot 1 = 1,\ 1 \cdot i = i \cdot 1 = i,\ i^2 = -1. \tag{2}$$

Oni diras, ke $F(z)$ estas analitika en malfermita domajno E, se $F(z)$ estas derivebla (monogena) en ĉiu punkto de E.

Ĝeneraligo. La ideo nature venas demandi al si, kiun klason de funkcioj oni ricevos, se oni adoptas en la prezentado regulon de multiplikado, kiu estas pli ĝenerala ol (2). Tio estas ideo, kiun ni aplikis en pluraj notoj kaj traktaĵoj, kaj kiu ankaŭ estas la bazo de tiu ĉi traktaĵo.

[1]) Vidu la liston de cititaj traktaĵoj sur p. 41.

[2]) Ni diras, ke $F(z)$ estas diferencialebla ĉe la punkto z se $P(x, y)$ kaj $Q(x, y)$ estas diferencialeblaj ĉe la punkto x, y.

Sed dum ni unue konsideris nur la kazojn de funkcioj de du aŭ tri realaj variantoj (Fréchet, [4], [5]), ni poste (Fréchet, [6], [7]) mallonge prezentis ĝeneraligon al *la kazo de n dimensioj*. Estas tiu kazo, kiun ni volas elvolvi nun.

Ĉiu leganto, kiu konas la teorion de la „hiperkompleksaj" nombroj rekonos, ke la ĝeneraligo, kiun ni elvolvos poste, konsistas en anstataŭigo, por la kampoj de variado de z kaj $F(z)$, de la kampo de la ordinaraj kompleksaj nombroj (kiu havas du dimensiojn) per la kampo de hiperkompleksaj nombroj (kiu havas ajnan nombron da dimensioj).

Tamen, por igi tiun ĉi traktaĵon legebla por pli granda nombro da legantoj, *ni nenie postulas konon pri la teorio de la hiperkompleksaj nombroj*. Ni uzos nur la plej elementan vektoranalizon kaj la fundamentajn ecojn de la klasikaj analitikaj funkcioj.

Ni observu, ke la formulo (1) povas esti interpretata en la jena maniero:

Oni povas konsideri z kaj $F(z)$ kiel du vektorojn, kiuj situacias en la (x, y)-ebeno kaj kiuj havas la respektivajn projekciojn x kaj y, P kaj Q. Se oni signas per e_1, e_2 du unuovektorojn sur la aksoj (ortaj aŭ oblikvaj) ox, oy, oni ricevas la *vektorajn* egalaĵojn

$$z = x\,e_1 + y\,e_2,\quad F(z) = P(x, y)\,e_1 + Q(x, y)\,e_2.$$

Oni povas diri, ke $Z = F(z)$ difinas *vektoran transformon* kaj ke $F(z)$ estas monogena (aŭ derivebla) transformo ĉe $z = z^0$ $(z^0 = x^0 + iy^0)$, se

1° $F(z)$ estas diferencialebla ĉe $z = z^0$,

2° ekzistas vektoro $F'_0 = Ae_1 + Be_2$, *sendependa de dx kaj dy*, tia ke

$$[dF(z)]_{z=z^0} = F'_0 \cdot dz, \tag{3}$$

t. e. tia, ke

$$(dP)_{\substack{x=x^0\\y=y^0}}\,e_1 + (dQ)_{\substack{x=x^0\\y=y^0}}\,e_2 = (A\,e_1 + B\,e_2)\cdot(dx\,e_1 + dy\,e_2)$$

kun la konvencio ke

$$e_1^2 = e_1,\ e_1 \cdot e_2 = e_2 = e_2 \cdot e_1,\ e_2^2 = -e_1. \tag{4}$$

Tiam la vektoro F'_0 estas la derivaĵo (vektora) de la funkcio (vektora) $F(v)$ ĉe $v = v^0$.

Sed prezentinte tiun difinon de la monogenaj (aŭ deriveblaj) funkcioj (Fréchet, [2]), ni atentigis, ke ĝi postulas, por esti korekta, difinon de la diferencialebleco de P kaj Q pli malvastan ol tiu, kiu konsistas en la ekzisto de iliaj parcialaj derivaĵoj. Oni devas supozi, ke P kaj Q estas diferencialeblaj en la senco unue proponita de Stolz kaj poste sendepende de W. H. Young.

Sed anstataŭ difini nerekte la diferencialon de $F = P + iQ$ per la diferencialoj de P kaj Q metante apriore $dF = dP + i\,dQ$, oni povas difini dF rekte, aplikante en la kazo de ebena spaco la difinon de la diferencialo, kiun ni donis aliloke (Fréchet, [3]) por spacoj pli ĝeneralaj ol la eŭklida spaco.

Anstataŭ apliki tiun difinon en la kazo de ebena spaco, ni tuj transiros al la kazo de n dimensioj.

Kazo de *n*-dimensiaj spacoj. En analogio al la kazo de la ebeno ni konsideros transformon $V = F(v)$ de vektoro v varianta en n-dimensia kartezia spaco, t_n, al vektoro V en la sama spaco. Ni rilatigu tiun spacon al n aksoj, ortaj aŭ oblikvaj. Estu $e_1, e_2, \ldots, e_n$ n unuovektoroj lokigitaj sur tiuj aksoj, kaj estu $x_1, \ldots, x_n$, $X_1, \ldots, X_n$ la projekcioj de v kaj V sur tiuj aksoj. Ni havas la egalaĵojn *vektorajn*

$$v = x_1\,e_1 + \cdots + x_n\,e_n, \tag{5}$$

$$V = X_1\,e_1 + \cdots + X_n\,e_n. \tag{6}$$

Kaj la egalaĵo *vektora*

$$V = F(v)$$

tradukiĝas per la skalaraj egalaĵoj

$$(7) \qquad X_1 = F_1(x_1, \ldots, x_n), \ \ldots, \ X_n = F_n(x_1, \ldots, x_n).$$

Derivado laŭ $x_1 \ldots, x_n$. Antaŭ ol doni la difinon de la paraanalitikaj funkcioj, ni difinos pli ĝeneralan klason de funkcioj, kiu havas sian propran intereson.

La formulo (3) povas formale esti skribata kun la novaj simboloj jene:

$$(8) \qquad [dF(v)]_{v=v_0} = V'_0 \cdot dv.$$

Sed por ke tiu formulo havu sencon estas necese, antaŭe doni du difinojn:

1º difinon de la produto de du vektoroj de t_n. Tiu produto devas mem esti vektoro en t_n.

2º difinon de la diferencialo de vektora funkcio V en t_n kies argumento v apartenas al t_n.

Vektora produto. Koncerne 1º oni vidas, ke kiel speciala kazo oni devas difini ĉiun produton $e_k \cdot e_r$ kiel vektoro de t_n. Oni do *devas* havi egalaĵojn *vektorajn* de la formo

$$(9) \qquad e_k \cdot e_r = \sum_{h=1}^{n} u_{krh}\, e_h$$

el kiu rezultas ĝenerala egalaĵo de la formo

$$(10) \qquad (\sum \xi_k\, e_k) \cdot (\sum x_r\, e_r) = \sum_h \Big(\sum_k \sum_r \xi_k\, x_r\, u_{krh}\Big) e_h.$$

(Oni revenas tie ĉi al la simboloj de la teorio de la hiperkompleksaj nombroj, sed oni ne bezonas koni tiun teorion.)

La formuloj (9) kaj (10) difinas *regulon R de vektora multipliko*, determinitan per la sistemo u_{krh} de realaj konstantoj.

Vektora diferencialo. Aplikante nian ĝeneralan difinon de la diferencialo (Fréchet, [3]) ni diras, ke la vektora funkcio $F(v)$ de la vektoro v estas diferencialebla por $v = v^0 = x_1^0 e_1 + \cdots + x_n^0 e_n$, se ekzistas lineara vektora funkcio $L[\Delta v]$ de la vektora kresko Δv de v, tiel ke oni havas

$$(11) \qquad \Delta F = L[\Delta v] + \| \Delta v \| \, \varepsilon,$$

kie

$$\Delta F = F(v^0 + \Delta v) - F(v^0),$$

kie $\| \Delta v \|$ signas „normon" de Δv, kaj kie ε estas vektoro tia ke

$$\lim_{\| \Delta v \| \to 0} \| \varepsilon \| = 0.$$

Por $\| \Delta v \|$ ni povas preni ajnan „normon" de Δv. Se oni rilatigas la vektorojn al n ortaj aŭ oblikvaj aksoj, v havas la projekciojn $x_1, \ldots, x_n$ kaj oni povas meti ekzemple

$$\| \Delta v \| = | \Delta x_1 | + \cdots + | \Delta x_n |, \quad \text{aŭ} \quad \| \Delta v \| = \sqrt{(\Delta x_1)^2 + \cdots + (\Delta x_n)^2}.$$

Aliflanke oni povas, sur la bazo de niaj ĝeneralaj difinoj de polinomoj de donita grado en tre ĝeneralaj spacoj, (Fréchet, [1]), montri, ke lineara vektorfunkcio de Δv necese estas *vektoro* $L(\Delta v)$ kies projekcioj estas de la formo

$$c_{11}\, \Delta x_1 + \cdots + c_{n1}\, \Delta x_n, \ldots, c_{1n}\, \Delta x_1 + \cdots + c_{nn}\, \Delta x_n.$$

$L(\Delta v)$ estas nomata la *diferencialo* de $F(v)$ ĉe $v = v^0$ kaj estas signata per $(dF)_{v=v^0}$.

Se $F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots x_n)$ estas la projekcioj de $F(v)$, $\varepsilon_1, \ldots, \varepsilon_n$ la projekcioj de ε, la *vektora* egalaĵo (11) estas ekvivalenta al la sistemo, kiu konsistas el n skalaraj egalaĵoj de la formo

$$\Delta F_h(x_1, \ldots, x_n) = (c_{1h}\,\Delta x_1 + \cdots + c_{nh}\Delta x_n) + \varepsilon_h \,\|\, \Delta v \,\|,$$

kun $\lim\limits_{\|\Delta v\| \to 0} \varepsilon_h = 0$.

Oni facile vidas, ke tiam F_h devas havi parcialajn derivaĵojn ĉe la punkto $x_1^0, \ldots, x_n^0$, kaj ke oni havas

$$c_{kh} = \left[\frac{\partial}{\partial x_k} F_h(x_1, \ldots, x_r)\right]_{v=v^0},$$

tiel, ke

$$\Delta F_h(x_1, \ldots, x_n) = \sum_k \left[\frac{\partial F_h(x_1, \ldots, x_n)}{\partial x_k}\right]_{v=v^0} \Delta x_k + \varepsilon_k \,\|\, \Delta v \,\|,$$

kun $\lim\limits_{\|\Delta v\| \to 0} \varepsilon_h = 0$.

Oni tiam revenas al la difino de Stolz-W. H. Young, kaj oni povas diri: por ke la vektora funkcio $F(v)$ estu diferencialebla ĉe $v = v^0$, estas necese kaj sufiĉe, ke ĉiu projekcio de $F(v)$ estu diferencialebla (en la senco de Stolz-W. H. Young) ĉe $v = v^0$. Kaj tiam la diferencialo de $F(v)$ havas kiel projekciojn la diferencialojn de la projekcioj de $F(v)$

$$dF(v) = dF_1(x_1, \ldots x_n)\, e_1 + \cdots + dF_n(x_1, \ldots, x_n)\, e_n$$

$$dF_h(x_1, \ldots, x_n) = \frac{\partial F_h}{\partial x_1} dx_1 + \cdots + \frac{\partial F_h}{\partial x_n} dx_n.$$

Speciale

$$dv = dx_1\, e_1 + \cdots + dx_n\, e_n$$

La uzo de tiuj difinoj de la diferencialo havas kiel ĉefan avantaĝon establi perfektan paralelecon inter la ecoj de diferencialoj de funkcioj de unu varianto kaj la ecoj de diferencialoj de funkcioj de pluraj variantoj. Tiu paraleleco ne troviĝis ĉe la pli fruaj difinoj. (Tiu paralelismo estis precizigata de W. H. Young [11] kaj per ni [3]). La samaj difinoj havas aliflanke la avantaĝon lumigi la econ (kiu estas esenca en fizikaj kaj aliaj aplikoj) de la diferencialo esti speco de ĉefparto de la kresko de la funkcio kaj esti simpla funkcio de la kreskoj de la variantoj.

Vektora derivado rilate al regulo de vektora multipliko. Ni diros nun, ke vektorfunkcio $V = F(v)$ estas *derivebla* ĉe $v = v^0$, *rilate al donita regulo* R de vektora multipliko, se

1º $F(v)$ estas diferencialebla (*en senco kiun ni ĵus precizigis*) ĉe $v = v^0$,

2º ekzistas vektoro V_0' de t_n *sendependa de* dv tia, ke oni havas, kiam oni aplikas la regulon R

$$[dF(v)]_{v=v^0} = V_0' \cdot dv. \tag{12}$$

Cetere, kiam la regulo R estas arbitra, $V_0' \cdot dv$ povas esti diversa de $dv \cdot V_0'$. En la kazo de formulo (12) oni do devas precizigi, dirante, ke $F(v)$ estas *maldekstre* derivebla ĉe $v = v^0$. En analogio $F(v)$ estas *dekstre* derivebla, se oni havas

$$[dF(v)]_{v=v^0} = dv \cdot V_0' \tag{13}$$

kaj simple *derivebla*, se $F(v)$ estas derivebla kaj dekstre kaj maldekstre kun la sama derivaĵo.

Ekzemplo. Ekzistas funkcio, kiu estas derivebla rilate al ĉiu regulo R de multipliko, nome vektorfunkcio, kiu estas konstanta. Ĉar se oni reprezentas per O la vektoron, kies ĉiuj projekcioj estas nulaj

$$O = 0\, e_1 + \cdots + 0\, e_n$$

oni havas, se $F(v)$ estas konstanta vektoro, $\Delta F(v) = O$, $dF(v) = O$, kaj sekve, kiaj ajn estas la konstantoj u_{krh}

$$dF(v) = O \cdot dv = dv \cdot O$$

do $F(v)$ estas derivebla rilate al ajna regulo de multipliko kaj havas la derivaĵon O.

Rimarko. Ĝenerala studo de la (dekstre aŭ maldekstre) derivebla funkcioj rilate al ajna regulo R de multipliko povas havi sian intereson. Ni montris tion en la kazo de du dimensioj en antaŭa traktaĵo (Fréchet, [8]).

Limigoj. Sed se oni volas, ke la funkcioj derivebla rilate al R havu multajn analogiojn kun la analitikaj funkcioj, estas necese submeti R al kelkaj limigoj.

Ni notu unue inter la ecoj de la analitikaj funkcioj la jenajn:

Se $f_1(z), f_2(z), f_3(z)$ estas analitikaj ĉe $z = z_0$, oni havas

$$f_1(z)\, f_2(z) = f_2(z)\, f_1(z),$$

$$[f_1(z)\, f_2(z)]\, f_3(z) = f_1(z)\, [f_2(z)\, f_3(z)].$$

Analogie ni postulos, ke la regulo R estu tia, ke se $F_1(v), F_2(v), F_3(v)$ estas derivebla rilate al R ĉe $v = v^0$, oni havas

$$F_1(v) \cdot F_2(v) = F_2(v) \cdot F_1(v), \tag{14}$$

$$[F_1(v) \cdot F_2(v)] \cdot F_3(v) = F_1(v) \cdot [F_2(v) \cdot F_3(v)]. \tag{15}$$

Tio speciale devas esti vera, kiam $F_1(v), F_2(v), F_3(v)$ estas konstantaj vektorfunkcioj. Por ajnaj vektoroj v, w, z de t_n oni do devas havi

$$v \cdot w = w \cdot v,$$

$$(v \cdot w) \cdot z = v \cdot (w \cdot z).$$

Estas tio, kion oni esprimas, kiam oni diras, ke la regulo R devas esti *komuteca* kaj *asocieca*. Evidente tiu necesa kondiĉo ankaŭ sufiĉas por ke la egalaĵoj (14), (15) estu plenumitaj por kiaj ajn vektoraj funkcioj (derivebla aŭ ne) $F_1(v)$, $F_2(v)$, $F_3(v)$. Krome rezultas el la komuteco, ke la distingo inter dekstra kaj maldekstra derivâjo malaperas.

Aliflanke oni scias, ke la speciala funkcio z estas analitika ĉie. Analoge ni elektos la regulon R tiel ke la vektorfunkcio $J(v) \equiv v$ estas derivebla rilate al R. Oni evidente havas $dJ(v) = dv$. Por ke $J(v)$ estu derivebla rilate al R ĉe $v = v^0$, necesas kaj sufiĉas, ke ekzistu vektoro I tia, ke

$$dv = dJ(v) = I \cdot dv = dv \cdot I.$$

Ĉar dv estas arbitra vektoro, oni vidas, ke devas ekzisti vektoro I de t_n, tia, ke oni havas por ajna vektoro w de t_n

$$I \cdot w = w \cdot I = w.$$

Se I' estas alia vektoro, kiu verigas la saman kondiĉon

$$I' \cdot w = w \cdot I' = w,$$

oni havas

$$I \cdot I' = I' \cdot I = I' \quad \text{kaj} \quad I' \cdot I = I \cdot I' = I,$$

do $I' = I$. Ekzistas do ne pli ol unu tia vektoro. Oni nomas ĝin *ĉefvektoro* rilate al la regulo R.

Ni kontentiĝas certigi tiujn tri analogiojn, ĉar kiel ni vidos, ili sufiĉos por sekvigi multajn aliajn.

Parakompleksaj vektoroj. Fine, *ni limigos nin de nun* al la kazo, kiam la regulo R de vektora multipliko (difinita per egalaĵo de la formo (9)) verigas la jenajn tri kondiĉojn:

La regulo R estas komuteca kaj asocieca.

Ekzistas ĉefvektoro por la regulo R.

Se vektoroj estas submetitaj al regulo de multipliko, kiu verigas tiujn tri kondiĉojn, ni nomas ilin *parakompleksaj vektoroj*. Kaj *ni distingigos* la regulojn, kiuj verigas tiujn tri kondiĉojn *per la simbolo* R_p.

Unikeco de la derivaĵo. Se $F(v)$ havus du derivaĵojn V_0' kaj W_0' ĉe $v = v^0$, oni havus la egalaĵojn

$$W_0 \cdot dv = [dF(v)]_{v=v^0} = V_0' \cdot dv, \tag{16}$$

sekve

$$(W_0' - V_0') \cdot dv = O. \tag{17}$$

Kiam $F(v)$ estas parakompleksa funkcio (kies argumento estas parakompleksa varianto kun la sama regulo de multipliko), oni povas preni por dv la ĉefvektoron I. Tiam (17) donas

$$W_0 - V_0' = (W_0' - V_0') \cdot I = O, \text{ tial } W_0' = V_0'.$$

La derivaĵo ĉe $v = v^0$ de derivebla *parakompleksa* vektorfunkcio do estas *unika*. Oni povas precizigi ĝian esprimon. Por fari tion ni metos ankaŭ $dv = I$ en (16). Se $I = \sum_r I_r e_r$, ni ricevas

$$V_0' \cdot I = [dF(v)]_{\left\{\substack{v=v^0\\ dv=I}\right\}} = \sum_h \left[\sum_r \frac{\partial F_h}{\partial x_r} I_r\right] e_h,$$

sekve

$$\boxed{V_0' = \sum_h \left[\sum_r I_r \frac{\partial}{\partial x_r} F_h(x_1^0, \ldots, x_n^0)\right] e_h.} \tag{18}$$

Pli simpla esprimo por V_0'. Se oni rilatigas la spacon t_n al aliaj aksoj sen ŝanĝo de la origino, oni ekhavas novajn unuovektorojn, kiuj estas ligitaj al la malnovaj unuovektoroj per formuloj tiaj, ke

$$e_h' = a_{h1} e_1 + \cdots + a_{hn} e_n$$

kie la determinanto $\{a_{hk}\}$ de la koeficientoj estas nenula. Ĉar la transformo estas unu-unu-senca, oni povas skribi

$$e_k = a_{k1}' e_1' + \cdots + a_{kn}' e_n'.$$

El tio ni ricevas

$$\begin{aligned} e_h' \cdot e_j' &= \left(\sum_l a_{hl} e_l\right) \cdot \left(\sum_m a_{jm} e_m\right) \\ &= \sum_l \sum_m a_{hl} a_{jm} \sum_k u_{lmk} e_k \\ &= \sum_l \sum_m \sum_k \sum_p a_{hl} a_{jm} u_{lmk} a_{kp}' e_p', \end{aligned}$$

kiu estas egalaĵo de la formo

$$e_h' \cdot e_j' = \sum_q u_{hjq}' e_q',$$

kiu estas de la sama formo kiel la responda egalaĵo por la e_k (sed kun aliaj koeficientoj).

Oni povas profiti de tio prenante la ĉefvektoron $I = e_1$. Se

$$I = \sum I'_h e'_h$$

oni do ricevas

$$I'_1 = 1, \quad I'_2 = \cdots = I'_n = 0.$$

Oni tiel ricevas la plej simplan esprimon por la derivaĵo. Metante

$$v = \sum_k y_k e'_k, \quad v^0 = \sum_k y^0_k e'_k, \quad F(v) = \sum_h G_h(y_1, \ldots, y_n) e'_h,$$

oni ricevas el (18) por la derivaĵo $G'(v^0)$ de $G(v)$

$$G'(v^0) = \sum_h \left[\frac{\partial}{\partial y_1} G_h(y_1, \ldots, y_n)\right]_{v=v^0} e'_h \tag{19}$$

aŭ pli mallonge

$$G'(v^0) = \left[\frac{\partial}{\partial y_1} G(v)\right]_{v=v^0}. \tag{19 bis}$$

Ecoj de certaj familioj de vektorfunkcioj. Ni indikos ecojn de ĝeneralaj parakompleksaj vektorfunkcioj, poste de tiuj el ili, kiuj estas deriveblaj, fine de tiuj, kiujn ni poste nomos paraanalitikaj. Pluraj el ili ŝajnas tro evidentaj por meriti esti menciataj, tamen ŝajnas al ni necese precizigi ilin, por establi interligon inter la diversaj kategorioj de vektorfunkcioj kaj la koncepto de „trioperacia algebro" de Karl Menger [10], koncepto kiun ni prezentos poste, p. 29 (cetere ni poste aldonos aliajn ecojn al tiuj, kiuj difinas la trioperacian algebron).

Ecoj de la parakompleksaj vektorfunkcioj. Se $F(v)$, $G(v)$, $H(v)$ estas parakompleksaj funkcioj submetitaj al la sama regulo R_p de multipliko, kaj difinitaj en la ĉirkaŭaĵo de la sama vektoro v^0, rezultas evidente el la kondiĉoj metitaj sur R_p, ke oni havas

$$\begin{gathered} F + G = G + F, \ (F + G) + H = F + (G + H), \\ F \cdot G = G \cdot F, \ (F \cdot G) \cdot H = F \cdot (G \cdot H), \\ (F + G) \cdot H = F \cdot H + G \cdot H. \end{gathered} \tag{20}$$

Estu $L(z)$, $M(w)$ ankaŭ parakompleksaj funkcioj submetitaj al la regulo R_p. Ili estu difinitaj en la ĉirkaŭaĵoj de la vektoroj w^0, z^0, kun

$$w^0 = F(v^0), \quad z^0 = M(v^0).$$

Ni nomos *substituo* la operacion, kiu kondukas de $F(v)$ al $M(F(v))$ kaj de $M(w)$ al $L(M(w))$, kun — se ekzemple

$$w = \sum_k y_k e_k \quad \text{kaj} \quad M(w) = \sum_h M_h(y_1, \ldots, y_n) e_h \ —$$

la vektora egalaĵo

$$M(F(v)) = \sum_h M_h(F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots, x_n)) e_h.$$

Estas klare, ke $M(F(v))$ estas difinita en la ĉirkaŭaĵo de v^0 kaj $L(M(w))$ en la ĉirkaŭaĵo de w^0. Kaj la substituo estas operacio, kiu ne necese estas komuteca, sed evidente ĉiam *asocieca*: Ĝi donas la saman rezulton, kiam oni substituas $M(F(v))$ en $L(z)$ kaj kiam oni substituas $F(v)$ en $L(M(w))$.

Plue la substituo estas *distribueca* rilate al adicio. Tio signifas, ke, se $N(w)$ ankaŭ estas parakompleksa funkcio difinita en la ĉirkaŭaĵo de w^0, oni povas ricevi la sumon $M(F(v)) + N(F(v))$ aŭ en la maniero, ke oni unue substituas F en M kaj N kaj adicias la rezultojn, aŭ en la maniero, ke oni unue adicias M kaj N kaj substituas F en tiun sumon.

Simile la substituo ankaŭ estas *distribueca rilate al multipliko.* Tio signifas, ke $M(F(v)) \cdot N(F(v))$ povas esti trovata aŭ en la maniero, ke oni unue substituas F en M kaj N kaj poste multiplikas, aŭ en la maniero, ke oni unue formas la produton $M(w) \cdot N(w)$ kaj poste substituas $F(v)$.

Inter la parakompleksaj funkcioj troviĝas la konstantaj vektorfunkcioj O kaj I kaj la funkcio $J(v) \equiv v$. Oni evidente havas

$$(21) \quad F(v) + O = F(v), \; F(v) \cdot I = F(v), \; F(J(v)) = J(F(v)) = F(v),$$

$$(22) \quad F(v) + [-F(v)] = O$$

kaj

$$(23) \quad O \neq I \neq J(v) \neq O.$$

Fine estas klare, ke substituo de konstanta vektorfunkcio $O(v)$ en konstantan vektorfunkcion $I(v)$ ne ŝanĝas la lastan funkcion

$$(24) \quad I(O(v)) = I(v).$$

Ĉiuj rimarkoj de tiu ĉi paragrafo estas banalaj, sed kiel ni diris pli frue, ili havas la celon montri, ke oni povas uzi la „trioperacian algebron" de Karl Menger [10], en la priskribota maniero.

Trioperacia algebro. Karl Menger diras, ke elementoj $F, G, H, \ldots$ de ajna naturo apartenantaj al certa amaso Q estas submetitaj al trioperacia algebro kiam

1º oni difinis tri operaciojn nomitajn adicio, multipliko, substituo, el kiuj ĉiu asocias determinitan elementon de Q al ajna paro F, G de elementoj el Q. La rezultojn de la tri operacioj oni signas respektive per $F + G$, $F \cdot G$, FG;

2º oni signas per O, I, J tri specialajn elementojn de Q, kaj oni asocias al ĉiu elemento F de Q determinitan elementon de Q, kiun oni reprezentas per $-F$;

3º la amaso Q kaj la tri operacioj verigas la kondiĉojn (aŭ aksiomojn) prezentatajn en la jena tabelo

Trioperacia algebro de Karl Menger

Kondiĉoj el kiuj ĉiu rilatas unu solan operacion

Adicio	Multipliko	Substituo
$F + G = G + F$ $(F + G) + H = F + (G + H)$ $F + O = F$ $F + (-F) = O$	$F \cdot G = G \cdot F$ $F \cdot (G \cdot H) = (F \cdot G) \cdot H$ $F \cdot I = I \cdot F = F$	$(FG)H = F(GH)$ $FJ = JF = F$

Tiu tabelo postulas la ekziston de specialaj elementoj O, I, J de la konsiderata amaso Q, kiuj krome estas submetitaj al la kondiĉo

$$O \neq I \neq J \neq O.$$

Kondiĉoj el kiuj ĉiu rilatas du operaciojn

$(F \cdot G) H = (FH) \cdot (GH)$	$(F + G) H = FH + GH$	$(F + G) \cdot H = F \cdot H + G \cdot H$

Estas esence rimarki, ke en tiu tabelo Karl Menger *ne* supozas, ke la elementoj F, G, H, J estas funkcioj, kaj ke la vorto substituo estas nur pro la analogio de la ecoj,

kiujn li atribuas al tiu operacio kun la ecoj de la ordinara operacio de substituo de unu funkcio en alian funkcion.

Se oni prenus por amaso Q la parakompleksajn vektorfunkciojn difinitajn en la ĉirkaŭaĵo de vektoro v^0 kaj por la tri operacioj: la vektoran adicion, la vektoran multiplikon difinitan per fiksa regulo R_p, kaj la substituon en la ordinara senco (t. e. kiel sur p. 28), oni povus diri, ke la kondiĉoj de la tabelo, kiuj ne enhavas la substituon, estas plenumitaj. Sed la situacio *ne estus la sama koncerne la substituon*, ĉar ĝi enmiksus funkciojn, kiuj ne necese estus difinitaj en la ĉirkaŭaĵo de la sama punkto v^0.

Kontraŭe, se oni *prenas por amaso* Q la vektorfunkciojn difinitajn *en la tuta spaco* t_n, oni povas diri, ke *ili estas submetitaj al trioperacia algebro en la senco de Karl Menger.*

Ecoj de la deriveblaj parakompleksaj vektorfunkcioj.

En la sekvo estos ofte konvene signi per DF la derivaĵon de $F(v)$ ĉe $v = v^0$.

Estu $\mathfrak{D}$ la familio de la parakompleksaj vektorfunkcioj $F(v)$, kiuj estas deriveblaj ĉe $v = v^0$ rilate la saman regulon R_p.

Se $F(v)$, $G(v)$ apartenas al $\mathfrak{D}$, F kaj G estas deriveblaj ĉe $v = v^0$, do ankaŭ $F + G$ estas derivebla kaj ni havas

$$\{d[F(v) + G(v)]\}_{v=v^0} = [F'(v^0) + G'(v^0)] \cdot dv .$$

Sekve $F + G$ *ankaŭ apartenas* al $\mathfrak{D}$ *kaj*

$$D(F + G) = DF + DG . \tag{25}$$

Same $F \cdot G$ estas derivebla ĉe $v = v^0$. Ĉar

$$F \cdot G = \sum_h \sum_k \sum_r u_{hkr} F_h(x_1, \ldots, x_n) G_k(x_1, \ldots, x_n) e_r ,$$

$$d(F \cdot G) = \sum_h \sum_k \sum_r u_{hkr} [F_h dG_k + (dF_h) G_k] e_r = F \cdot dG + G \cdot dF .$$

Sekve

$$d(F \cdot G) = F \cdot (G' \cdot dv) + G \cdot (F' \cdot dv) = (F \cdot G' + G \cdot F') \cdot dv .$$

Do $F \cdot G$ *ankaŭ apartenas* al $\mathfrak{D}$ *kaj*

$$D(F \cdot G) = F \cdot DG + G \cdot DF . \tag{26}$$

Se $F(v)$ apartenas al $\mathfrak{D}$ kaj se $M(w)$ estas derivebla rilate al la sama regulo R_p kiel $F(v)$ en la ĉirkaŭaĵo de $w^0 = F(v^0)$, oni ricevas

$$[d M(w)]_{w=w^0} = M_0' \cdot dw , \quad [d F(v)]_{v=v^0} = F_0' \cdot dv .$$

Se oni prenas por w, $F(v)$, oni do ricevas

$$[d M(F(v))]_{v=v^0} = M_0' \cdot F_0' \cdot dv ,$$

tial $M(F(v))$ estas *derivebla* ĉe $v = v^0$, rilate al R_p, kiel estas $F(v)$, kaj ĝia derivaĵo estas $M_0' \cdot F_0'$. Oni povas skribi

$$D(MF) = (DM) F \cdot F' . \tag{27}$$

Estas klare, ke la konstantoj O, I estas deriveblaj kaj oni vidis, ke $J(v) \equiv v$ ankaŭ estas derivebla. O, I, J do apartenas al $\mathfrak{D}$ kaj ankaŭ plenumas la kondiĉojn (21), (22), (23), (24).

Kiam F, G, H apartenas al la familio $\mathfrak{D}$ ne nur validas ankoraŭ la egalaĵoj (20), sed rezultas de la antaŭe dirita, ke tiuj de iliaj kombinaĵoj, kiuj troviĝas en (20), ankaŭ

apartenas al $\mathfrak{D}$. Plue, la substituo, kiu restas asocieca kaj distribueca rilate al kaj la multipliko kaj la adicio, ĝenerale ne estas komuteca.

Fine oni vidas, ke se oni prenas por amaso Q la amason de ĉiuj parakompleksaj vektorfunkcioj, kiuj estas deriveblaj *en la tuta spaco* t_n, rilate la saman regulon R_p, tiuj funkcioj estas *submetitaj al la trioperacia algebro* de Karl Menger.

Aliaj ecoj de la funkcioj, kiuj estas deriveblaj rilate R_p. La deriveblaj funkcioj estas solvoj de sistemoj de parcialaj diferencialaj ekvacioj.

1° *Sistemo de la unua ordo.* Kiam oni kombinas (16) kaj (18) oni vidas, ke oni havas

$$\sum_h dF_h(x_1, \ldots, x_n)\, e_h = \left\{\sum_k \left[\sum_\varrho I_\varrho \frac{\partial F_k(x_1, \ldots, x_n)}{\partial x_\varrho}\right] e_k\right\} \cdot \left(\sum_r dx_r\, e_r\right)$$

sekve

$$\boxed{\frac{\partial}{\partial x_r} F_h(x_1, \ldots, x_n) = \sum_k \left[\sum_\varrho I_\varrho \frac{\partial F_k(x_1, \ldots, x_n)}{\partial x_\varrho}\right] u_{krh}} \tag{28}$$

kie h, r, k, ϱ prenas la valorojn de 1 al n. Se do $\sum_h F_h(x_1, \ldots, x_n)\, e_h$ reprezentas parakompleksan vektorfunkcion, kiu estas derivebla rilate al R_p, ĉe $v = v^0 = x_1^0 e_1 + \cdots + x_n^0 e_n$, la funkcioj F_h verigas sistemon (28) de parcialaj diferencialaj ekvacioj, kiuj estas de la unua ordo, linearaj, homogenaj kaj kun konstantaj koeficientoj.

Tiu sistemo enhavas n^2 ekvaciojn. Sed kiam oni prenas la akson, kiu portas la vektoron I kiel akson ox_1, la sistemo fariĝas la jena sistemo S

$$S: \quad \boxed{\frac{\partial F_h}{\partial x_r} = \sum_{k=1}^{n} u_{krh} \frac{\partial F_k}{\partial x_1}, \quad \text{kie} \begin{cases} r = 2, \ldots, r \\ h = 1, 2, \ldots, r \end{cases}} \tag{29}$$

en kiu n ekvacioj, kie $r = 1$, reduktiĝas al identaĵoj. En la resto de la sistemo, la derivaĵoj laŭ $x_2, \ldots, x_n$ estas esprimitaj per la derivaĵoj laŭ x_1.

Fine oni vidas, ke oni *ĝeneraligas gravan econ* de la klasikaj analitikaj funkcioj, kiam oni konkludas: *la n komponantoj $F_h(x_1, \ldots, x_n)$ de parakompleksa vektorfunkcio, kiu estas derivebla en punkto $v^0 = \Sigma x_k^0 e_k$ rilate al la regulo R_p, verigas en la punkto $(x_1^0, \ldots, x_n^0)$ sistemon de parcialaj diferencialaj ekvacioj de la unua ordo, kiuj estas linearaj, homogenaj, kaj kun konstantaj koeficientoj. Tiu sistemo estas algebre reduktebla al $n^2 - n$ ekvacioj (kaj ne al malpli ol $n^2 - n$ ekvacioj)*

2° *Sistemo de parcialaj diferencialaj ekvacioj de la dua ordo.* Ni konsideru la kazon kiam la parakompleksa vektorfunkcio $F(v)$ ne nur estas derivebla rilate al R_p en la ĉirkaŭaĵo de v^0, sed ankaŭ havas diferencialon de la dua ordo ĉe $v = v^0$. Oni vidis, ke se oni prenas ox_1 sur la akso kiu portas I, oni havas en la ĉirkaŭaĵo de v^0

$$\frac{\partial F_h}{\partial x_r} = \sum_k u_{krh} \frac{\partial F_k}{\partial x_1} \qquad \text{(por } r = 1 \text{ oni havas identaĵojn).}$$

Oni povas derivi denove laŭ x_s kaj ricevas

$$\frac{\partial^2 F_h}{\partial x_r \partial x_s} = \frac{\partial}{\partial x_1} \sum_k u_{krh} \sum_q \frac{\partial F_q}{\partial x_1} u_{qsk}$$

aŭ

$$\frac{\partial^2 F}{\partial x_r \partial x_s} = \sum_q \left(\sum_k u_{qsk}\, u_{krh}\right) \frac{\partial^2 F_q}{\partial x_1^2}. \tag{30}$$

Pro la asocieco de R_p oni havas

$$\left[\left(\sum_q x_q e_q\right)\cdot\left(\sum_s y_s e_s\right)\right]\cdot\left(\sum z_r e_r\right) = \left(\sum x_q e_q\right)\cdot\left[\left(\sum y_s e_s\right)\cdot\left(\sum z_r e_r\right)\right]$$

aŭ

$$\sum x_q y_s z_r \sum_h \left(\sum_k u_{qsk} u_{krh}\right) e_h = \sum x_q y_s z_r \sum_h \left(\sum_k u_{qkh} u_{srk}\right) e_h$$

sekve

$$\sum_k u_{qsk} u_{krh} = \sum_k u_{qkh} u_{srk} \,. \tag{31}$$

Do

$$\frac{\partial^2 F_h}{\partial x_r \partial x_s} = \sum_k u_{srk}\left(\sum_q u_{qkh} \frac{\partial^2 F_q}{\partial x_1^2}\right).$$

Speciale, ĉar $e_s \cdot e_1 = e_s$ kaj tial $u_{s1k} = \delta_{sk}$ oni havas

$$\frac{\partial^2 F_h}{\partial x_1 \partial x_s} = \sum_k \delta_{sk} \sum_q u_{qkh} \frac{\partial^2 F_q}{\partial x_1^2} = \sum_q u_{qsh} \frac{\partial^2 F_q}{\partial x_1^2}$$

aŭ

$$\frac{\partial^2 F_h}{\partial x_1 \partial x_k} = \sum_q u_{qkh} \frac{\partial^2 F_q}{\partial x_1^2}$$

sekve

$$\frac{\partial^2 F_h}{\partial x_r \partial x_s} = \sum_k u_{srk} \frac{\partial^2 F_h}{\partial x_1 \partial x_k} \,. \tag{32}$$

Cetere ni notas, ke por $r = 1$ la formulo fariĝas identaĵo, same por $s = 1$. Aliflanke la koeficientoj estas sendependaj de h.

Ni do vidas, ke *la komponantoj* $F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots, x_n)$ *de parakompleksa vektorfunkcio* $F = \sum_h F_h e_h$, *kiu estas derivebla rilate al regulo* R_p *en la ĉirkaŭaĵo de* v^0 *kaj dufoje diferencialebla por* $v = v^0$, *verigas, ĉe* $v = v^0$, *la saman sistemon* σ *de* $\frac{n(n-1)}{2}$ *parcialaj diferencialaj ekvacioj de la dua ordo, kiuj estas linearaj, homogenaj kaj kun konstantaj koeficientoj* (kiuj estas unike determinitaj per la regulo R_p), kaj kiuj enhavas unu solan nekonatan funkcion U

$$\sigma: \quad \boxed{\frac{\partial^2 U}{\partial x_r \partial x_s} = \sum_k u_{srk} \frac{\partial^2 U}{\partial x_1 \partial x_k}} \qquad (r > 1, s > 1)\,. \tag{33}$$

Plue tiuj ekvacioj estas *algebre sendependaj*, se oni komprenas per tio, ke kiam oni substituas por la $\frac{\partial^2 U}{\partial x_r \partial x_s}$ sendependajn variantojn y_{rs}, oni ricevas sendependajn ekvaciojn. Ĉar ili estas solvitaj laŭ la y_{1k}.

Efektive nia demonstracio ne validas rekte, krom en la kazo kiam e_1 estas la ĉefvektoro. Sed oni pasas de la ĝenerala kazo al tiu kazo per ŝanĝo de aksoj. Se oni operacias en la inversa direkto, oni vidas, ke la F_h verigas sistemon de $\frac{n(n-1)}{2}$ ekvacioj, kiuj ankoraŭ estas algebre sendependaj kaj kiuj havas la ĝeneralan formon

$$\sum_{r,s} a_{rs} \frac{\partial^2 U}{\partial y_r \partial y_s} = 0\,. \tag{34}$$

Tial tio, kiu estas kursive presita, restas valida por ajna regulo R_p.

Primitiva vektorfunkcio. Estu $F(v) = \sum_h F_h(x_1, \ldots, x_n)\, e_h$ parakompleksa vektorfunkcio, kiu estas derivebla en la ĉirkaŭaĵo de $v^0 = \sum x_r^0\, e_r$. Ĉu ekzistas funkcio de la sama naturo, $\varphi(v)$, kiu havas $F(v)$ kiel derivaĵo laŭ la sama regulo R_p?

Por simpligi ni prenos la akson, kiu portas I kiel ox_1. Laŭ (19bis) ni havas

$$F(v) = \varphi'(v) = \frac{\partial \varphi(v)}{\partial x_1}.$$

Oni do unue devas trovi funkciojn φ_h tiajn, ke

$$F_h(x_1, \ldots, x_n) = \frac{\partial}{\partial x_1}\, \varphi_h(x_1, \ldots, x_n).$$

Ĉar la F_h estas diferencialeblaj, ili estas kontinuaj, ekzistas do funkcioj ψ_h tiaj, ke

$$F_h = \frac{\partial \Psi_h}{\partial x_1}.$$

Oni do havas

$$\varphi_h(x_1, \ldots, x_n) = \psi_h(x_1, \ldots, x_n) + \Theta_h(x_2, \ldots, x_n).$$

Ni volas, ke φ estu de la sama naturo kiel F, do derivebla rilate al la sama regulo R_p kiel F. Oni do devas havi

$$\frac{\partial \varphi_h}{\partial x_r} = \sum u_{krh} \frac{\partial \varphi_k}{\partial x_1}, \quad r > 1,$$

kaj sekve la Θ_h devas verigi la sistemon

$$\frac{\partial \Theta_h(x_2, \ldots, x_n)}{\partial x_r} = \lambda_{h,r}(x_1, \ldots, x_n) \tag{35}$$

kie

$$\lambda_{h,r}(x_1, \ldots, x_n) = \sum_k u_{krh} \frac{\partial \Psi_k(x_1, \ldots, x_n)}{\partial x_1} - \frac{\partial \Psi_h(x_1, \ldots, x_n)}{\partial x_r}.$$

Oni havas

$$\frac{\partial \lambda_{h,r}}{\partial x_1} = \sum_k u_{krh} \frac{\partial^2 \Psi_k}{\partial x_1^2} - \frac{\partial^2 \Psi_h}{\partial x_1 \partial x_r} = \sum_k u_{krh} \frac{\partial F_k}{\partial x_1} - \frac{\partial F_h}{\partial x_r} = 0.$$

La λ_h do estas sendependaj de x_1. Oni devas integri sistemon de la formo

$$\frac{\partial \Theta_h(x_2, \ldots, x_n)}{\partial x_r} = \mu_{hr}(x_2, \ldots, x_n) \quad \text{kun} \begin{cases} h = 1, \ldots, n \\ r = 2, \ldots, n. \end{cases} \tag{35 bis}$$

Se tiu sistemo havas solvon, oni ricevas ĉiun alian solvon aldonante al la Θ_h arbitrajn konstantojn. Por ke la sistemo (35 bis) havu solvon necesas kaj sufiĉas, ke la μ_{hr} verigas kondiĉojn de integrebleco de la formo

$$\frac{\partial \mu_{hr}}{\partial x_s} = \frac{\partial \mu_{hs}}{\partial x_r}.$$

Tio signifas, ke

$$\begin{aligned} 0 &= \frac{\partial}{\partial x_s}\left[\sum_k u_{krh} \frac{\partial \Psi_k}{\partial x_1} - \frac{\partial \Psi_h}{\partial x_r}\right] - \frac{\partial}{\partial x_r}\left[\sum_k u_{ksh} \frac{\partial \Psi_k}{\partial x_1} - \frac{\partial \Psi_h}{\partial x_s}\right] \\ &= \frac{\partial}{\partial x_s} \sum_k u_{krh} F_k - \frac{\partial}{\partial x_r} \sum_k u_{ksh} F_k \\ &= \sum_k u_{krh}\left(\sum_q \frac{\partial F_q}{\partial x_1} u_{qsk}\right) - \sum_k u_{ksh}\left(\sum_q \frac{\partial F_q}{\partial x_1} u_{qrk}\right) \\ &= \sum_q \left[\sum_k (u_{krh}\, u_{qsk} - u_{ksh}\, u_{qrk})\right] \frac{\partial F_q}{\partial x_1}. \end{aligned}$$

Sed se oni permutas s kaj q en (31) oni ricevas

$$\sum_k u_{sqk}\, u_{krh} - \sum_k u_{qrk}\, u_{skh} = 0\,,$$

kaj ĉar R_p estas komuteca, la kondiĉoj de integrebleco estas plenumitaj.

Resume, *ekzistas parakompleksa vektorfunkcio $\varphi(v)$, kiu estas derivebla rilate al R_p en la ĉirkaŭaĵo de v^0 kaj kiu estas unika* — se oni malatentas adician konstantan vektoron — *tiel, ke la derivaĵo $\varphi'(v)$ de $\varphi(v)$ rilate al R_p en la ĉirkaŭaĵo de v^0 estas egala al arbitre donita funkcio $F(v)$ de la sama naturo.* Oni povas nomi $\varphi(v)$ *primitiva* vektorfunkcio de $F(v)$.

Integralo. Se oni konsideras rektifeblan kontinuan kurbon Γ, kiu kunligas du punktojn A kaj B en la spaco t_n, kaj parakompleksan vektorfunkcion $F(v)$, kiu estas derivebla rilate al R_p en ĉiu punkto de Γ, oni povas kalkuli la laŭkurban integralon en la senco de Stieltjes

$$\int_\Gamma F \cdot dv = \sum_h \left[\int_\Gamma \sum_k \sum_r F_k(x_1, \ldots, x_n)\, u_{krh}\, dx_r \right] e_h$$

kie la x_r estas kontinuaj funkcioj de parametro, kiu povas esti la arkolongo. Tiu integralo do havas determinitan signifon kaj reprezentas determinitan vektoron $\sum_h A_h\, e_h$.

Laŭ la antaŭe dirita F havas primitivan funkcion $\varphi(v)$, kiu estas unika (se oni malatentas adician konstantan vektoron). Oni do havas

$$\int_\Gamma F \cdot dv = \int_\Gamma d\varphi = \varphi(B) - \varphi(A)\,. \tag{36}$$

Estu $F(v)$ derivebla rilate al R_p ne nur sur Γ sed ankaŭ en domajno D en kies interno Γ troviĝas. Se la primitiva funkcio estas unuforma, oni vidas, ke la integralo dependas nur de la ekstremaĵoj A kaj B. Kaj se la kurbo Γ estas fermita, la integralo estas nula.

Simplaj ekzemploj de parakompleksaj vektorfunkcioj, kiuj estas derivebla rilate al R_p. I. Estas klare, ke ĉiu konstanta parakompleksa vektorfunkcio estas derivebla rilate al ajna regulo R_p kaj por ĉiu vektoro v. Ĉar se $F(v)$ estas konstanta, oni povas skribi

$$\Delta F(v) = O = O \cdot dv = dv \cdot O\,,$$

kaj la derivaĵo de $F(v)$ estas O[3]), kiel ni jam vidis supre.

II. Estas same pri la vektorfunkcio $J(v) = v$, ĉar

$$dJ(v) = dv = I \cdot dv = dv \cdot I\,.$$

La derivaĵo de J do estas la ĉefvektoro I (ni ankaŭ vidis tion).

El la antaŭe dirita sekvas. ke se c_0, c_1 estas konstantaj vektoroj

$$c_0 \cdot v + c_1$$

estas ankaŭ derivebla, ĉar ĝi estas ricevita per adicio kaj multipliko de derivebla funkcioj. Pro la sama kaŭzo estas same pri

$$(c_0 \cdot v + c_1) \cdot v + c_2 = c_0 \cdot v^2 + c_1 \cdot v + c_2$$

k. t. p., kaj ĝenerale pri la funkcio

$$c_0 \cdot v^q + c_1 \cdot v^{q-1} + \cdots + c_{q-1}\, v + c_q$$

---

[3]) Se sur malfermita amaso E de t_n, $F(v)$ estas derivebla kaj se ĝia derivaĵo estas nula, ĝia diferencialo ankaŭ estas nula. Oni tiam scias, ke se E estas koneksa, $F(v)$ estas konstanta sur E.

kie $c_0, c_1, \ldots, c_q$ estas parakompleksaj nombroj kiel v. Tiun funkcion ni nomas *parakompleksa polinomo de grado* $\leqq q$. Resume: *Ĉiu polinomo parakompleksa rilate al regulo R_p estas derivebla rilate al R_p por ajna vektoro v kaj por ajna grado de la polinomo.*

Laŭ la formuloj de derivado (25), (26), oni havas

$$D(c_0 \cdot v + c_1) = c_0 \cdot Dv = c_0 \cdot I = c_0 ,$$

$$D[(c_0 \cdot v + c_1) \cdot v + c_2] = (c_0 \cdot v + c_1) \cdot Dv + v \cdot D(c_0 \cdot v + c_1) = 2c_0 \cdot v + c_1$$

kaj procedante per paŝoj

$$\begin{aligned} D(c_0 \cdot v^q + c_1 \cdot v^{q-1} + \cdots + c_q) &= c_0 \cdot q v^{q-1} + c_1 \cdot (q-1) v^{q-2} + \cdots \\ &= q c_0 \cdot v^{q-1} + (q-1) c_1 \cdot v^{q-2} + \cdots + 2c_{q-2} \cdot v + c_{q-1} . \end{aligned} \tag{37}$$

III. Parakompleksa polinomo estas derivebla rilate al ajna regulo R_p. Kontraŭe nia dua ekzemplo koncernas *regulon specialan* de multipliko R_p^0, laŭ kiu

$$e_k \cdot e_r = \begin{cases} e_k & \text{se } k = r \\ 0 & \text{se } k \neq r . \end{cases} \tag{38}$$

Tiam oni ricevas

$$\left(\sum_k V'_k e_k\right) \cdot \left(\sum_r dx_r e_r\right) = \sum_k V'_k dx_k e_k .$$

Se do $F(v) = \sum_k F_k e_k$ estas derivebla rilate al R_p^0, kaj havas ĉe $v = v^0$ la derivaĵon

$$V' = \sum_k V'_k e_k$$

oni devas havi

$$d\left(\sum_k F_k e_k\right) = \sum_k V'_k dx_k e_k$$

sekve

$$dF_k = V'_k dx_k .$$

Se do $v = \sum_k x_k e_k$, $F_k(x_1, \ldots, x_n)$ devas esti funkcio de nur x_k, kaj tiu funkcio devas esti diferencialebla ĉe $v = v^0 = \sum_k x_k^0 e_k$. Tio signifas, ke $F_k = F_k(x_k)$, kie $F_k(x_k)$ estas derivebla ĉe $x_k = x_k^0$.

Inverse, ĉiu parakompleksa vektorfunkcio $F(v)$ *de la formo*

$$F(v) = \sum_k F_k(x_k) e_k$$

kie F_k estas derivebla ĉe $x_k = x_k^0$ *estas derivebla* ĉe $v = v^0$ *rilate al* R_p^0.

Limigo de la familio de derivebla vektorfunkcioj. Se parakompleksa vektorfunkcio $F(v)$ estas derivebla rilate al R_p en ĉirkaŭaĵo de v^0, ĝia derivaĵo $F'(v)$ estas bone difinita parakompleksa funkcio en tiu ĉirkaŭaĵo. Sed la derivaĵo ne necese estas derivebla rilate al R_p ĉe $v = v^0$. Estas eĉ eble, ke ĝi ne estas diferencialebla ĉe $v = v^0$.

Sed unu el la plej gravaj ecoj de la klasikaj analitikaj funkcioj estas, ke la derivaĵo $f'(z)$ de funkcio $f(z)$, kiu estas analitika ĉe $z = z^0$, ankaŭ estas analitika ĉe $z = z^0$.

Por pligrandigi la analogion kun la klasikaj analitikaj funkcioj de la funkcioj, kiuj estas derivebla rilate al R_p, ni do estas kondukitaj al konsidero nur de konvene elektita subamaso $\mathfrak{P}$ de la amaso $\mathfrak{D}$ de la parakompleksaj vektorfunkcioj, kiuj estas derivebla rilate al R_p ĉe $v = v^0$. Kaj ni volas ĝin elekti en tia maniero, ke la derivaĵo $F'(v)$ de funkcio $F(v)$ de la amaso $\mathfrak{P}$ apartenas al $\mathfrak{P}$. Sed tiam $F'(v)$ mem havas derivaĵon $F''(v)$ ĉe $v = v^0$, k. t. p. Por ke oni povu paroli pri la derivaĵo de $F'(v)$ ĉe $v = v^0$, necesas unue ke $F'(v)$

estas difinita en ĉirkaŭaĵo de v^0. Same $F''(v)$ devas esti difinita en tiu ĉirkaŭaĵo, k. t. p. Tio postulas almenaŭ, ke $F(v)$ estu diferencialebla en la ĉirkaŭaĵo de v^0, ke estu same pri $F'(v)$, k. t. p. Fine, la amaso $\mathfrak{P}$, kiun ni volas difini, devas enhavi nur funkciojn, kiuj estas derivebla en la ĉirkaŭaĵo de v^0 kaj senfine diferencialeblaj en la ĉirkaŭaĵo de v^0. Tiuj kondiĉoj estas necesaj. Ni montros, ke ili estas sufiĉaj.

Paraanalitikaj vektorfunkcioj. Ni nomas *paraanalitika vektorfunkcio ĉe $v = v^0$ rilate al la regulo R_p* ĉiun parakompleksan vektorfunkcion, kiu en ĉiu punkto de ĉirkaŭaĵo $\mathfrak{V}$ de v^0 estas

1º *senfine diferencialebla*[4])

2º *derivebla rilate al la regulo R_p.*

La amason de tiuj funkcioj por fiksa regulo R_p ni prenas kiel amason $\mathfrak{P}$. Por ĉiu funkcio $F(v)$ de $\mathfrak{P}$, ĝia derivaĵo estas difinita en la ĉirkaŭaĵo $\mathfrak{V}$. Ni volas montri, ke $F'(v)$ ankaŭ apartenas al $\mathfrak{P}$:

La derivaĵo de paraanalitika vektorfunkcio ĉe v^0 rilate al regulo R_p, ankaŭ estas paraanalitika vektorfunkcio ĉe v^0 rilate al la sama regulo R_p.

Efektive oni vidis, ke

$$F'(v) = \sum_h \left[\sum_\varrho I_\varrho \frac{\partial F_h}{\partial x_\varrho} \right] e_h . \tag{39}$$

1º Do ĉar la F_h estas senfine diferencialeblaj en $\mathfrak{V}$ estas same pri $F'(v)$.

2º Laŭ (28) ni devas pruvi, ke en ĉiu punkto de $\mathfrak{V}$ oni havas

$$\frac{\partial F'_h}{\partial x_r} = \sum_k \left(\sum_\mu I_\mu \frac{\partial F'_k}{\partial x_\mu} \right) u_{krh} . \tag{40}$$

Nu, laŭ (39)

$$F'_k = \sum_\varrho I_\varrho \frac{\partial F_h}{\partial x_\varrho} .$$

Estas do necese, ke

$$\sum_\varrho I_\varrho \frac{\partial^2 F_h}{\partial x_r \partial x_\varrho} = \sum_k \left[\sum_\varrho I_\varrho \left(\sum_\lambda I_\lambda \frac{\partial^2 F_k}{\partial x_\varrho \partial x_\lambda} \right) \right] u_{krh} , \tag{41}$$

sed oni havas

$$\frac{\partial F_h}{\partial x_r} = \sum_k \left(\sum_\lambda I_\lambda \frac{\partial F_k}{\partial x_\lambda} \right) u_{krh}$$

sekve, per kombinado oni ricevas (41).

Simplaj ekzemploj de paraanalitikaj vektorfunkcioj.

I. Rezultas senpere de p. 35 ke: *ĉiu parakompleksa vektora polinomo*

$$c_0 \cdot v^q + c_1 \cdot v^{q-1} + \cdots$$

estas paraanalitika en ĉiu punkto rilate al ajna regulo R_p.

II. Aliflanke rezultas ankaŭ de p. 35 ke *ĉiu parakompleksa vektorfunkcio de la formo*

$$F(v) = \sum_h F_h(x_h)\, e_h$$

[4]) Estas tamen ne sen intereso konsideri paraanalitikajn funkciojn en pli ĝenerala senco, kie la regulo de multipliko ne necese estas submetita al la 3 kondiĉoj de la p. 34/35 kaj kie la kondiĉo 1º ĉisupre estas forigata. Efektive estas tiu pli ĝenerala difino, kiun ni studis en la kazo de du dimensioj kaj kiu kondukis al sufiĉe frapaj rezultoj.

kie $F_h(x_h)$ estas *senfine derivebla en la ĉirkaŭaĵo de* x_h^0, estas *paraanalitika* ĉe $v = v^0 = \Sigma x_h^0 e_h$ *rilate al la regulo* R_p^0 de p. 35. Kaj inverse, ĉiu funkcio, kiu estas paraanalitika ĉe $v = v^0$ rilate al tiu regulo R_p^0 estas de la formo indikita ĉi-supre.

Aliaj ekzemploj. Ni nun donos aliajn ekzemplojn, kiuj postulas antaŭirantan teorion pri *vektoraj potencoserioj*. Por tiu celo ni unue establos kelkajn lemojn.

Lemoj. I. Estu v, w ajnaj du parakompleksaj vektoroj. La kvociento $\dfrac{\| v \cdot w \|}{\| v \| \, \| w \|}$ havas finitan superanton kiam $v \neq 0$, $w \neq 0$. Kaj tio validas por ajna normo se nur $\| v + w \| \leqq \| v \| + \| w \|$, $\| cw \| = | c | \, \| w \|$ por ĉiu reala nombro c;

$$\| e_h \| = 1, \; | x_h | \leqq \| \Sigma x_k e_k \| .$$

Tiuj kondiĉoj estas plenumitaj ekzemple kiam

$$\| \Sigma x_k e_k \| = \sqrt{\Sigma x_k^2} \text{ aŭ kiam } \| \Sigma x_k e_k \| = \Sigma | x_k | .$$

Oni tiam havas

$$\| v \cdot w \| = \| \sum_{k,r,h} u_{krh} v_k w_h e_h \| \leqq \sum_h | \sum_{k,r} u_{krh} v_k w_r |$$
$$\leqq n^2 \sum_h \| v \| \, \| w \| \Big(\sum_{k,r} | u_{krh} \Big) = N_0 \| v \| \, \| w \| .$$

II. Estu $v_1, v_2, \ldots, v_p$ p parakompleksaj vektoroj. Oni havas

$$\| v_1 \cdot v_2 \| \leqq N_0 \| v_1 \| \, \| v_2 \| ;$$
$$\| v_1 \cdot v_2 \cdot v_3 \| \leqq N_0 \| v_1 \| \, \| v_2 \cdot v_3 \| \leqq N_0^2 \| v_1 \| \, \| v_2 \| \, \| v_3 \|$$

kaj ĝenerale

$$\| v_1 \cdot v_2 \cdot \cdots v_q \| \leqq N_0^{q-1} \| v_1 \| \, \| v_2 \| \cdots \| v_q \| < N^q \| v_1 \| \, \| v_2 \| \cdots \| v_n \|,$$

se oni metas $N = N_0 + 1$. Speciale

$$\| v^q \| \leqq N^q \| v \|^q . \tag{42}$$

III. Oni vidis (p. 35), ke v^q estas derivebla, kun

$$dv^q = q v^{q-1} \Delta v \quad \text{kaj} \quad \Delta v^q = dv^q + \| \Delta v \| \, \varepsilon_q, \quad \text{kie} \lim_{\| \Delta v \| \to 0} \varepsilon_q = 0 .$$

Ni volas trovi superantan funkcion por $\| \varepsilon_q \|$. Oni havas

$$\| \Delta v \| \, \| \varepsilon_q \| = \| (v + \Delta v)^q - v^q - q v^{q-1} \cdot \Delta v \| = \| \mu \| .$$

Se oni metas $v + \Delta v = v'$, oni havas

$$\begin{aligned} \mu &= (v + \Delta v)^q - v^q - q v^{q-1} \cdot \Delta v \\ &= (v' - v) \cdot [v'^{q-1} + v \cdot v'^{q-2} + \cdots + v^{q-1} - q v^{q-1}] \\ &= (v' - v) \cdot [(v'^{q-1} - v^{q-1}) + v \cdot (v'^{q-2} - v^{q-2}) + \cdots] \\ &= (\Delta v)^2 \cdot \{v'^{q-2} + v \cdot v'^{q-3} + \cdots + v^{q-2} + v \cdot (v'^{q-3} + v \cdot v'^{q-4} + \cdots) + \cdots\} \end{aligned}$$

Se do $\| v \| < \varrho$ kaj $\| v + \Delta v \| < \varrho$,

$$\| \mu \| < N^q \| \Delta v \|^2 \{\varrho^{q-2}((q-1) + (q-2) + \cdots + 1)\}$$
$$= N^q \varrho^{q-2} \frac{q(q-1)}{2} \| \Delta v \|^2$$

kaj sekve, por $\| \Delta v \| \neq 0$,

$$\| \varepsilon_q \| \leqq N^q \varrho^{q-2} \frac{q(q-1)}{2} \| \Delta v \| , \tag{43}$$

kiam $\| v \| < \varrho$ kaj $\| v + \Delta v \| < \varrho$.

IV. *Konverĝo de vektoraj serioj.* Estu

$$v^{(1)} + v^{(2)} + \cdots + v^{(q)} + \cdots \tag{44}$$

formala serio de vektoroj de t_n. Ni diras, ke tiu serio konverĝas al sumo S, se oni havas

$$\lim_{q \to \infty} \| v^{(1)} + \cdots + v^{(q)} - S \| = 0 .$$

En tiu kazo oni evidente havas

$$\| v^{(q)} \| \leqq \| v^{(1)} + \cdots + v^{(q)} - S \| + \| v^{(1)} + \cdots + v^{(q-1)} - S \| .$$

Tial, se serio de vektoroj konverĝas, ĝia ĝenerala termo konverĝas al O.

Simpla kazo, kie la konverĝo de la vektora serio (44) estas certigita, estas tiu, kie la *nombra* serio de ĝiaj normoj

$$\sum \| v^{(q)} \|$$

konverĝas. Efektive, en tiu kazo, se

$$v^{(q)} = \sum_k x_k^{(q)} e_k ,$$

oni havas

$$| x_k^{(q)} + \cdots + x_k^{(q+r)} | \leqq | x_k^{(q)} | + \cdots + | x_k^{(q+r)} | \leqq \| v^{(q)} \| + \cdots + \| v^{(q+r)} \| .$$

La lasta membro konverĝas al nul, kiam q kreskas senfine, tial ankaŭ la unua membro konverĝas al nul. La nombra serio $\sum_q x_k^{(q)}$ do konverĝas por ĉiu valoro de k, sekve ankaŭ la serio (44) konverĝas. En tiu ĉi kazo ni diros, ke la serio (44) konverĝas *absolute*.

Parakompleksaj potencaj vektoraj serioj. Ni konsideru la formalan potencan vektoran serion

$$a_0 + a_1 \cdot v + \cdots + a_q \cdot v^q + \cdots \tag{45}$$

kie la a_k kaj v estas parakompleksaj vektoroj submetitaj al la sama regulo R_p. Oni vidis, ke

$$\| a_q \cdot v^q \| \leqq N^q \| a_q \| \| v \|^q .$$

Sekve, se la *nombra* serio

$$\sum \| a_q \| (N \| v \|)^q$$

konverĝas, ankaŭ la *vektora* serio (45) konverĝas, ni diru al $S(v)$. Se ϱ_0 estas la konverĝoradiuso de la serio

$$\| a_0 \| + \| a_1 \| \varrho + \cdots + \| a_q \| \varrho^q + \cdots , \tag{46}$$

la serio (45) estas konverĝa, eĉ absolute konverĝa, almenaŭ por $\| v \| < \frac{\varrho_0}{N}$. Se oni metas

$$\Delta(a_q \cdot v^q) = a_q \cdot \Delta v^q = q a_q \cdot v^{q-1} \cdot \Delta v + \| \Delta v \| a_q \cdot \varepsilon_q ,$$

oni havas laŭ la lemo III

$$\| a_q \cdot \varepsilon_q \| \leqq \frac{N^3 q(q-1)}{2} (N\varrho)^{q-2} \| a_q \| \| \Delta v \|$$

por $\| v \| < \varrho$, $\| v + \Delta v \| < \varrho$. Estu $0 < \varrho < \varrho_0$. Por $\| v \| < \frac{\varrho}{N} (< \varrho)$, la serio $\sum_p a_p \cdot v^p$ konverĝas. Por $\| \Delta v \| < \frac{\varrho}{N} - \| v \|$ la serio $\sum_q a_q \cdot (v + \Delta v)^q$ ankaŭ konverĝas. Estas do same pri

$$\sum_q \Delta(a_q \cdot v^q) = S(v + \Delta v) - S(v) .$$

Oni havas

$$\| q a_q \cdot v^{q-1} \cdot \Delta v \| \leqq q N^{q+1} \| a_q \| \| v \|^{q-1} \| \Delta v \|$$
$$\leqq N^2 \| \Delta v \| (q \| a_q \| \varrho^{q-1}) .$$

Tial

$$\sum_q q a_q \cdot v^{q-1} \cdot \Delta v$$

ankaŭ konverĝas. Oni do povas skribi

$$S(v + \Delta v) - S(v) = (\sum_q q a_q \cdot v^{q-1}) \cdot \Delta v + \| \Delta v \| \varepsilon \tag{47}$$

kun

$$\| \varepsilon \| = \| \sum_q a_q \varepsilon_q \| .$$

Laŭ la lemo III oni ricevas

$$\| \varepsilon \| \leqq N^3 \left\{ \sum_q \frac{q(q-1)}{2} \| a_q \| N^{q-2} \varrho^{q-2} \right\} \| \Delta v \| .$$

Ĉar la serio $\sum_q \| a_q \| \varrho^q$ konverĝas por $\varrho < \varrho_0$, estas same pri ĝia dua derivaĵo $\sum_q q(q-1) \| a_q \| \varrho^{q-2}$. La esprimo inter krampoj do konverĝas por $\varrho < \varrho_0$. Por fiksa $\varrho < \varrho_0$ oni do povas skribi

$$\| \varepsilon \| < H \| \Delta v \| , \tag{48}$$

kie H estas sendependa de Δv kaj sekve

$$\lim_{\|\Delta v\| \to 0} \| \varepsilon \| = 0 .$$

Rezultas do de (47) kaj (48), ke la *sumo de la potenca vektora serio* (45), kiu konverĝas almenaŭ por $\| v \| < \frac{\varrho_0}{N}$, kaj en tiu sferoido reprezentas determinitan parakompleksan vektorfunkcion, *estas*, en la sama sferoido, *vektorfunkcio derivebla* (rilate al la regulo R_p). Kaj *ĝia derivaĵo egalas la sumon de la derivaĵoj de la termoj de tiu serio*

$$S'(v) = a_1 + a_2 \cdot v + \cdots + q a_q \cdot v^{q-1} + \cdots \tag{49}$$

La serio S' konverĝas kaj estas la derivaĵo de S almenaŭ en *la sama sferoido* $\| v \| < \frac{\varrho_0}{N}$.

Sed kiam oni aplikas la saman rezonadon al $S'(v)$, oni vidas, ke $S'(v)$ ankaŭ estas derivebla en la sama sferoido. Kaj tiel plu. Sekve $S(v)$ estas senfine derivebla en la sferoido.

Fine, oni vidas, ke se ϱ_0 estas la konverĝoradiuso de la nombra potencoserio

$$\sum_q \| a_q \| \varrho^q$$

kaj se $\varrho_0 > 0$, la vektora potencoserio

$$a_0 + a_1 \cdot v + \cdots + a_q \cdot v^q + \cdots$$

konverĝas almenaŭ interne de la sferoido

$$\| v \| < \frac{\varrho_0}{N} ,$$

kaj ke *ĝia sumo estas paraanalitika funkcio* almenaŭ interne de la sferoido.

Ĝeneraligo de la klasikaj funkcioj. Ni aplikos la antaŭe diritan al la specialaj potencoserioj

$$(50)\quad \begin{cases} I + I\cdot v + \frac{1}{2} I\cdot v^2 + \cdots + \frac{1}{q} I\cdot v^q + \cdots \\ I - \frac{1}{2} I\cdot v^2 + \frac{1}{4!} I\cdot v^4 + \cdots + \frac{(-1)^q}{(2q)!} I\cdot v^{2q} + \cdots \\ I\cdot v - \frac{1}{3!} I\cdot v^3 + \cdots + \frac{(-1)^q}{(2q+1)!} I\cdot v^{2q+1} + \cdots \end{cases}$$

Ĉar la serioj

$$1 + \varrho + \frac{\varrho^2}{2} + \cdots + \frac{\varrho^q}{q!} + \cdots,$$

$$1 + \frac{\varrho^2}{2} + \cdots + \frac{\varrho^{2q}}{(2q)!} + \cdots,$$

$$\varrho + \frac{\varrho^3}{3!} + \cdots + \frac{\varrho^{2q+1}}{(2q+1)!}$$

konverĝas por ajna ϱ, la tri vektoraj potencoserioj (50) konverĝas absolute por ajna v. Ili prezentas por ajna v tri paraanalitikajn funkciojn, kiujn ni povas signi per la simboloj e^v, kos v, sin v, pro analogio. Cetere oni povas forigi la termon I (kiun ni enkondukis por memorigi pri la skribmaniero $\sum_q a_q \cdot v^q$) en ĉiu termo, en kiu ĝi estas faktoro. Oni do povas skribi por ajna v

$$(51)\quad \boxed{\begin{aligned} e^v &= I + v + \frac{1}{2} v^2 + \cdots + \frac{1}{q!} v^q + \cdots \\ \text{kos } v &= I - \frac{1}{2} v^2 + \cdots + \frac{(-1)^q}{(2q)!} v^{2q} + \cdots \\ \sin v &= v - \frac{1}{3!} v^3 + \cdots + \frac{(-1)^q}{(2q+1)!} v^{2q+1} + \cdots \end{aligned}}$$

Laŭ la formulo (49) oni cetere vidas, ke oni havas

$$(52)\quad \boxed{\begin{aligned} de^v &= e^v \cdot dv, \\ d\,\text{kos } v &= -\sin v \cdot dv, \\ d \sin v &= \text{kos } v \cdot dv. \end{aligned}}$$

Evidente oni ankaŭ havas

$$(53)\quad \boxed{e^O = I,\ \text{kos } O = I,\ \sin O = O.}$$

Resume, la tri vektoraj potencoserioj (51) *konverĝas absolute por ajna vektoro v de la spaco t_n. Ili havas kiel respektivajn sumojn tri paraanalitikajn funkciojn por ajna v kaj por ajna regulo de multipliko R_p laŭ kiu la potencoj de v estas kalkulataj. Tiuj tri funkcioj verigas la klasikajn rilatojn* (52), (53), kiuj tie ĉi estas vektoraj rilatoj kalkulataj laŭ la regulo R_p.

Atentigo. Oni povus formuli ankoraŭ aliajn ecojn de la paraanalitikaj funkcioj ĝeneraligante aliajn ecojn de la klasikaj analitikaj funkcioj. Ni pensas, ke la antaŭe dirita sufiĉas por establi la analogion inter tiuj du kategorioj de funkcioj.

Aliflanke estas kompreneble, ke la analogio ne persistas por ĉiuj ecoj.

En alia traktaĵo (Fréchet [9]) ni konsideros pli speciale la kazon de paraanalitikaj funkcioj en malgranda nombro da dimensioj ($n = 2, 3, 4, \ldots$).

Listo de cititaj traktaĵoj.

[1] *M. Fréchet*, Sur la notion de différentielle totale, Nouv. Ann. Math , t. **12**, 1912, p. 385—403 et 433—449.

[2] *M. Fréchet*, Sur les conditions pour qu'une fonction $P(x, y) + iQ(x, y)$ soit monogène, Nouv. Ann. Math., t. **19**, 1919, p 215—219.

[3] *M. Fréchet*, La notion de différentielle dans l'Analyse générale, Ann. Ec. Norm. Sup., t. **42**, 1925, p. 293—323.

[4] *M. Fréchet*, Sur deux familles de fonctions analogues à la famille des fonctions analytiques, C. R., t. **235**, 1952, p. 1585—1587.

[5] *M. Fréchet*, Sur les fonctions paraanalytiques à 2 et à 3 dimensions, C. R., t. **236**, 1953 p. 348—351.

[6] *M. Fréchet*, Les fonctions paraanalytiques à n dimensions, C. R., t. **236**, 1953, p. 1832—1834.

[7] *M. Fréchet*, Propriétés des fonctions paraanalytiques à n dimensions, C. R., t. **236**, 1953, p. 2191—2194.

[8] *M. Fréchet*, Determinado de la plej ĝeneralaj planaj paraanalitikaj funkcioj, Annali di Matematica, t. **35**, 1953, p. 255—258.

[9] *M. Fréchet*, La kanonaj formoj de la 2-3-4 dimensiaj paraanalitikaj funkcioj, Compositio Mathematica.

[10] *Karl Menger*, Tri-operational Algebra, Reports of a Mathematical Colloquium, Second Series, Double issue 5—6, 1944, p. 3—10, Publication of the University Notre-Dame.

[11] *W. H. Young*, The fundamental theorems of the Differential Calculus, Cambridge tracts in Mathematics and Mathematical Physics n° 11, 1910.

Eingegangen 28. Januar 1954.

Über lineartopologische Algebren*).

Von *Friedhorst Ballier* in Mainz.

Einleitung.

Die Gesamtheit der linearen Abbildungen eines n-dimensionalen Vektorraumes L in seinen Grundkörper bildet einen zu L isomorphen Vektorraum L'. Der Wunsch, diese Symmetrieeigenschaft auf den unendlichdimensionalen Fall auszudehnen, führt im Zusammenhang mit ähnlichen Fragestellungen zur Untersuchung linearer Räume beliebiger Dimension (über beliebigem Grundkörper K), auf denen eine separierte lineare Topologie erklärt ist. Diese lineartopologischen Räume sind in [VIII]**), §§ 4—6, behandelt. Das natürliche Analogon für Algebren sind die lineartopologischen Algebren. Auf einer Algebra L über beliebigem Grundkörper K sei eine separierte Topologie T gegeben mit den folgenden Eigenschaften:

1. Es existiert eine Nullumgebungsbasis aus Subalgebren.
2. Die algebraischen Rechenoperationen sind stetig in T.
3. Die Umgebungen eines beliebigen Punktes $x \neq o$ aus L entstehen durch Translation um x aus den Nullumgebungen.

Dann nennen wir $L(T)$ eine *lineartopologische Algebra*. Es ist das Ziel der vorliegenden Arbeit, Eigenschaften dieser lineartopologischen Algebren zusammenzustellen. Eine entsprechende Aufgabe hatte sich E. Michael (vgl. [XI]) in seiner Dissertation gestellt, indem er, ausgehend von lokal konvexen Räumen, lokal multiplikativ-konvexe Algebren untersuchte. Es gelang ihm, diese Algebren in direkte Beziehung zu Banachalgebren zu setzen, so daß er deren Theorie zur Verfügung hatte. In unserem Fall muß eine solche Beziehungsnahme natürlich fehlen, weil wir uns nicht auf den Körper der komplexen Zahlen als Grundkörper beschränken. Vor allem das Fehlen des erweiterten Liouvilleschen Satzes (vgl. [IV], theorem 3. 12. 2) macht es oft unmöglich, sich der aus der Theorie der Banachalgebren bzw. aus [XI] bekannten Verfahren zu bedienen und analoge Ergebnisse zu erhalten. Wo eine Übertragung von Schlußweisen aus [XI] möglich war, wie im ersten und dritten Paragraphen, erscheinen die Resultate in einfacherer Form und nicht so weitgehend wie bei den lokal multiplikativ-konvexen Algebren. An Stelle analytischer Methoden treten rein algebraische bei allgemeinem Grundkörper.

In § 1 werden grundlegende Eigenschaften lineartopologischer Algebren abgeleitet und Beispiele gegeben. Der Begriff erweist sich invariant gegenüber den gebräuchlichsten topologischen und algebraischen Operationen wie Übergang zu einer Subalgebra, zur Restklassenalgebra nach einem abgeschlossenen, zweiseitigen Ideal, zum topologischen Produkt bzw. der topologischen direkten Summe oder zur vollständigen Hülle. Es ist dabei bereits mehrfach notwendig, statt der allgemeinen lineartopologischen Algebren die

*) Diese Arbeit wurde von der naturwissenschaftlichen Fakultät der Universität Mainz als Dissertation angenommen (D 77). Herrn Professor Dr. *Köthe* bin ich für mannigfache Anregungen und Ratschläge zu Dank verpflichtet.

**) Mit eingeklammerten römischen Zahlen verweise ich auf das Literaturverzeichnis am Schluß der Arbeit.

idealtopologischen Algebren zu betrachten. Solche Algebren sind der Untersuchung zugänglicher, weil in ihnen das Ringprodukt gleichmäßig stetig ist bezüglich beider Variablen. Diese charakterisierende Eigenschaft ist gleichbedeutend damit, daß es in $L(T)$ eine Nullumgebungsbasis aus zweiseitigen Idealen gibt (§ 1, Satz 1). In den nachfolgenden Sätzen wird der Begriff der *Quasiregularität* häufig verwendet. Wir gebrauchen ihn und die damit zusammenhängenden Bezeichnungen wie Radikal, Spektrum, im Sinn von Jacobson (vgl. [V]). Es werden hier einige Bemerkungen über Quasiregularität zusammengestellt, die wir später benötigen. Dann wenden wir uns zwei Darstellungsmöglichkeiten idealtopologischer Algebren zu. Eine solche Algebra kann als Subalgebra des topologischen Produktes diskreter Algebren L^i aufgefaßt werden. In Analogie zu [XI], theorem 5. 1, erhalten wir damit eine Charakterisierung vollständiger idealtopologischer Algebren als projektiven Limes (vgl. [XIII], chap. I, 5) der Faktoren L^i (siehe § 1, Satz 3). Eine der Folgerungen, die sich hieraus wie in [XI] ziehen lassen, zeigt, daß das Radikal einer vollständigen idealtopologischen Algebra abgeschlossen ist. Daneben ist jede idealtopologische Algebra Teil einer Algebra S von stetigen Endomorphismen in einem lineartopologischen Raum E (vgl. § 1, Satz 6); dabei wird auf S die Topologie der uniformen Konvergenz in E verwendet.

In § 2 betrachten wir *linear kompakte Algebren*, wobei der Begriff „linear kompakt" im Sinn von Lefschetz (vgl. [X], II, 6) zu verstehen ist. Linear kompakte Algebren sind immer idealtopologisch (§ 2, Satz 1). Aus [VIII] ist bekannt, daß die Topologie eines linear kompakten Raumes $L(T)$ stets die schwache Topologie T_s ist, welche mit Hilfe des dualen Raumes L' aller stetigen linearen Abbildungen von $L(T)$ in K erklärt ist. Während aber jeder lineartopologische Raum lineartopologisch ist auch bezüglich der schwachen Topologie, ergibt die Untersuchung der schwachen Topologie bei lineartopologischen Algebren, daß dies hier nicht mehr gilt. Es gibt lineartopologische Algebren $L(T)$, die bezüglich der schwachen Topologie nicht mehr lineartopologisch sind; als Beispiel nenne ich φ_d (für transfinites d), die topologische direkte Summe von d Summanden K (vgl. § 2, Satz 3). Die linear kompakten Algebren sind gerade die hinsichtlich T_s vollständigen lineartopologischen Algebren (§ 2, Satz 2, Korollar). Die in § 1 erhaltene Darstellung idealtopologischer Algebren als Teil eines topologischen Produktes kann für halbeinfache, linear kompakte Algebren genauer ausgeführt werden. Eine solche Algebra ist das topologische Produkt von vollen Matrizenalgebren endlichen Ranges über Schiefkörpern (§ 2, Satz 5)*). Es ergibt sich damit ein Analogon zum Wedderburnschen Struktursatz der klassischen Algebra. Wir ziehen verschiedene Folgerungen aus diesem Satz und gewinnen im Anschluß daran einen Struktursatz für halbeinfache, lokal linear kompakte Algebren (§ 2, Satz 7). Über das Radikal einer linear kompakten Algebra erhalten wir folgende Aussagen: Das Radikal R ist abgeschlossen, regulär, topologisch nilpotent und gleich dem Durchschnitt der R umfassenden offenen, maximalen zweiseitigen Ideale. Für eine kommutative linear kompakte Algebra L ist R die Gesamtheit der Elemente, deren n-te Potenzen gegen o konvergieren. Das Radikal einer lokal linear kompakten Algebra ist abgeschlossen (§ 2, Satz 8).

Der 3. Paragraph dient der Betrachtung lineartopologischer Algebren, für welche es „genügend viele" (algebraisch) homomorphe, stetige Abbildungen in den Grundkörper K gibt. Beispiele bieten φ_d und ω_d, das topologische Produkt von d Faktoren K. In diesen Fällen besteht die Gesamtheit $M(L)$ der stetigen, homomorphen Abbildungen von $L(T)$ in K gerade aus allen Projektionen p_i und der Nullabbildung Θ. Umgekehrt ist jede

*) Auf anderem Wege erhielt *D. Zelinsky* in [XIV], theorem 1, ein äquivalentes Ergebnis. Unser Beweis entstand in Anlehnung an den Beweis von *Kaplansky* für kompakte Ringe (vgl. [VI], theorem 16).

lineartopologische Algebra $L(T)$ algebraisch isomorph einer Subalgebra L^* von ω_d, wo d die Mächtigkeit von $M^-(L)$ (dies ist $M(L)$ ohne Θ) angibt; dabei gehen die Elemente aus $M^-(L)$ in die Projektionen von L^* über (§ 3, Satz 1). Derartige Algebren sind stets kommutativ und halbeinfach. Wir können L auch als Teilalgebra C_L der Menge $C_0(M(L))$ aller stetigen Abbildungen von $M(L)$ in K ansehen, welche für Θ verschwinden; auf $M(L)$ ist hierbei die schwache Topologie gewählt (§ 3, Satz 2). Ist $C_L = C_0(M(L))$, so sprechen wir von einer *vollen* lineartopologischen Algebra. Die Algebren φ_d, ω_d, allgemeiner das topologische Produkt und die topologische direkte Summe voller Algebren sind voll (§ 3, Satz 3). Wenn jede homomorphe Abbildung der vollen lineartopologischen Algebra $L(T)$ auf K stetig ist, dann ist $L(T)$ durch die topologischen Eigenschaften von $M(L)$ algebraisch bestimmt. Das Spektrum eines Elementes einer vollen lineartopologischen Algebra $L(T)$ besteht aus allen Skalaren $f(x)$, wo f über $M^-(L)$ läuft (§ 3, Satz 4). Wie der duale Raum L' zur Definition der schwachen Topologie auf L dient, so verwenden wir den Teilraum $M(L)$ von L', um eine neue Topologie T_F auf L einzuführen. T_F-vollständig sind gerade die in Analogie zu [IX], § 15, Satz 2, „vollkommen" genannten vollen Algebren (§ 3, Satz 5). Im Zusammenhang mit der Betrachtung der F-Topologie und der vollkommenen Algebren tritt schließlich die folgende Frage auf: Unter welchen Voraussetzungen über den separierten topologischen Raum E ist die Algebra $C_0(E)$ der für ein spezielles Element ξ_0 aus E verschwindenden stetigen Funktionen mit Werten in K bezüglich der Topologie der einfachen Konvergenz eine lineartopologische Algebra $L(T)$ mit $M(L) = E$? Wir finden als notwendige und hinreichende Bedingung, daß jedes Element in E eine Umgebungsbasis aus zugleich offenen und abgeschlossenen Mengen besitzt.

§ 1. Allgemeine Eigenschaften lineartopologischer Algebren.

Wir nennen einen linearen Raum L über diskretem Körper K *lineartopologisch*, wenn er eine solche separierte lineare Topologie besitzt, daß rx für $r \in K$, und $x + y$ stetige Funktionen von x bzw. von x und y sind. Dabei heißt eine Topologie *linear*, wenn eine Nullumgebungsbasis aus linearen Teilräumen existiert und wenn die Umgebungen eines beliebigen Punktes x von L durch Translation um x aus den Nullumgebungen entstehen. Der so erklärte *lineartopologische Raum* $L(T)$ ist ein uniformer Raum (vgl. [VIII], § 4).

Die besondere Struktur des lineartopologischen Raumes gestattet eine leichte Handhabung linearer Abbildungen:

(1) *Ist eine lineare Abbildung A eines lineartopologischen Raumes in einen ebensolchen in o stetig, so ist sie überall und sogar gleichmäßig stetig* (vgl. [VIII], § 4, 2).

Ferner gilt:

(2) *Ist U eine offene Menge eines lineartopologischen Raumes, so auch $M + U$ für beliebige Menge M; für eine lineare Nullumgebung U ist $M + U$ auch abgeschlossen* (vgl. [VIII], § 4, 2).

In Fortführung obiger Definition legen wir fest: $L(T)$ sei eine Algebra und ein lineartopologischer Raum; es gebe eine Basis (U_i), mit $i \in I$, der Nullumgebungen aus Subalgebren und xy sei stetig bezüglich jeder Variablen einzeln; dann heiße $L(T)$ eine *lineartopologische Algebra*. Die Indizesmenge I hat beliebige Mächtigkeit.

Es folgt sogleich:

(3) *In einer lineartopologischen Algebra ist die Ringmultiplikation stetig bezüglich beider Variablen zugleich.*

Denn sei die Umgebung $x_0y_0 + U_i$ von x_0y_0 gegeben. Wegen der Stetigkeit der Multiplikation in jedem Faktor einzeln gibt es Nullumgebungen U_k und U_l, so daß x_0U_k und $U_l y_0$ enthalten sind in U_i. Sei die Nullumgebung U_m in $U_i \cap U_k \cap U_l$ gelegen; für $(x, y) \in (x_0 + U_m, y_0 + U_m)$ ist dann $xy = x_0y_0 + x_0u_2 + u_1y_0 + u_1u_2$, wo die Elemente u_j in U_m liegen. Da wir U_i linear voraussetzen können, gehört xy zu $x_0y_0 + U_i$.

Während nach (1) in einem lineartopologischen Raum $L(T)$ die Addition immer eine gleichmäßig stetige Abbildung von $L \times L$ auf L darstellt, ist die gleichmäßige Stetigkeit des Ringproduktes nur bei einer im folgenden öfter auftretenden Klasse spezieller lineartopologischer Algebren erfüllt:

Satz 1. *Der lineartopologische Raum $L(T)$ sei eine Algebra und besitze eine Nullumgebungsbasis aus zweiseitigen Idealen U_i; dann ist $L(T)$ eine lineartopologische Algebra mit einem in beiden Variablen gleichmäßig stetigen Ringprodukt. Ist umgekehrt $L(T)$ eine lineartopologische Algebra mit einem in beiden Variablen gleichmäßig stetigen Ringprodukt, so hat $L(T)$ eine Nullumgebungsbasis aus zweiseitigen Idealen.*

Beweis. Eine Basis der uniformen Struktur von $L(T)$ ist gegeben in den Mengen N_i aller Elemente (x, y) aus $L \times L$, für welche $x - y$ in U_i liegt (vgl. [VIII], § 4, 2). Sei nun im 1. Fall ein festes offenes Ideal U_i vorgegeben. Für Elemente (x^1, y^1), (x^2, y^2) aus $L \times L$ mit $(x^1 - x^2) \in U_i$ und $(y^1 - y^2) \in U_i$ liegt dann $x^1y^1 - x^2y^2 = x^1(y^1 - y^2) + (x^1 - x^2)\, y^2$ in U_i, d. h. das Ringprodukt ist gleichmäßig stetig. — Um unsere 2. Behauptung nachzuweisen, müssen wir ein offenes, zweiseitiges Ideal in U_i finden, wenn nun U_i eine lineare Nullumgebung bedeutet. Nach Voraussetzung gibt es lineare Nullumgebungen $U_j < U_i$ und $U_k < U_i$, so daß aus $(x^1 - x^2) \in U_j$ und $(y^1 - y^2) \in U_k$ folgt $(x^1y^1 - x^2y^2) \in U_i$. Sei x ein beliebiges Element aus L; ist $x^1 = x^2 = x$, sowie $y^2 = o$ und bedeutet y^1 ein beliebiges Element aus U_k, so liegt also xy^1 in U_i, d. h. es ist $LU_k < U_i$. Ebenso gilt $U_j L < U_i$. Dieselbe Überlegung, für $U = U_j \cap U_k$ statt U_i ausgeführt, liefert eine lineare Nullumgebung $V < U$ mit den Eigenschaften $LV < U_i$, sowie $VL < U_i$ und $LVL < UL < U_i$; wenn wir durch Klammern die lineare Hülle kennzeichnen, so ist

$$W = V + (LV) + (VL) + (LVL)$$

ein offenes, zweiseitiges Ideal und enthalten in U_i. In ähnlichem Zusammenhang verweist Kaplansky auf diese Formel in [VI], I, Beweis von lemma 9.

Definition. Eine lineartopologische Algebra mit einer Nullumgebungsbasis aus zweiseitigen Idealen heißt eine *idealtopologische Algebra.*

Ein Beispiel bieten die diskreten Algebren:

(4) *Versieht man eine Algebra L mit der diskreten Topologie T, so ist $L(T)$ eine idealtopologische Algebra.*

Hier ist nämlich (o) eine Nullumgebungsbasis.

(5) *Umgekehrt ist offenbar jeder endlichdimensionale lineartopologische Raum diskret.*

Ein solcher diskreter lineartopologischer Raum ist stets vollständig, denn die uniforme Struktur ist ebenfalls diskret.

(6) *In einer idealtopologischen Algebra $L(T)$ ist jedes eigentliche, nicht in $L(T)$ dichte, (linke, rechte, zweiseitige) Ideal H in einem eigentlichen, offenen (und zugleich abgeschlossenen) Ideal (derselben Sorte) enthalten. Also ist jedes abgeschlossene, maximale Ideal auch offen.*

Beweis. Sei (U_i), mit $i \in I$, eine Nullumgebungsbasis aus zweiseitigen Idealen U_i. Da $\bar{H} \neq L$ ist, gibt es ein Element x in L und einen Index $i \in I$, so daß $H \cap (x + U_i)$

leer ist; daher liegt x nicht in dem offenen Ideal $H + U_i$, welches H enthält und von derselben Sorte wie H ist.

Wie ein lineartopologischer Raum konstruiert werden kann, zeigt folgender Satz:

(7) *Ist (U_i), mit $i \in I$, eine Filterbasis von linearen Teilräumen des linearen Raumes L mit Durchschnitt o, und führen wir auf L die lineare Topologie T ein, welche durch (U_i) als Umgebungsbasis von o erklärt ist, so ist L mit T ein lineartopologischer Raum* (vgl. [VIII], § 4, 2).

Ist L eine Algebra und sind die Mengen U_i zweiseitige Ideale in L, so ist $L(T)$ (nach Satz 1) eine idealtopologische Algebra.

Die Durchschnittsbedingung der Nullumgebungsbasis ist in jedem lineartopologischen Raum erfüllt; sie zeigt wegen (2), daß in einem solchen Raum die zusammenhängende Komponente eines Punktes dieser Punkt selbst ist, d. h. ein lineartopologischer Raum ist vollständig unzusammenhängend.

Mit Hilfe von (7) schließen wir:

Satz 2. *Seien eine Algebra L und eine Anzahl homomorpher Abbildungen f_i, mit $i \in I$, von L in lineartopologische Algebren L^i gegeben; für $x \neq y$ aus L gebe es ein i, so daß $f_i(x) \neq f_i(y)$ ist. Versieht man L mit der schwächsten Topologie T, in welcher alle Homomorphismen f_i stetig sind, so ist $L(T)$ eine lineartopologische Algebra. Im Fall idealtopologischer Algebren L^i ist auch $L(T)$ idealtopologisch.*

Beweis. (U_k^i), mit $k \in I_i$, sei eine lineare Nullumgebungsbasis von L^i. Die Gesamtheit $V = (V_l)$ bestehe aus allen Mengen $f_i^{(-1)}(U_k^i)$, mit $i \in I$ und $k \in I_i$, und deren endlichen Durchschnitten. V ist dann eine Filterbasis aus linearen Teilräumen von L, und zwar sind die Mengen V_l zweiseitige Ideale, wenn alle Mengen U_k^i es sind. Der Durchschnitt der linearen Teilräume V_l ist o, denn zu einem Element $x \neq o$ aus L gibt es nach Voraussetzung einen Homomorphismus f_i mit $f_i(x) \neq o$, also existiert eine Menge U_k^i, welche $f_i(x)$ nicht enthält; d. h. x ist nicht in $f_i^{(-1)}(U_k^i)$ enthalten. Die lineare Topologie T mit V als Nullumgebungsbasis macht L zu einem lineartopologischen Raum $L(T)$. Dabei sind die Umgebungen $x + V_l$ eines Elementes x aus L gerade die reziproken Bilder der Umgebungen $f_i(x) + U_k^i$ bzw. endliche Durchschnitte solcher Mengen; T ist also die gesuchte Topologie. $V_l V_l$ ist in V_l enthalten, weil alle Mengen U_k^i Algebren sind. Zum Nachweis der Stetigkeit von xy in $y = o$ geben wir uns eine Nullumgebung V_m vor. Ist V_m eine Menge $f_i^{(-1)}(U_k^i)$, so setzen wir $V_{l_m} = f_i^{(-1)}(U_{k'}^i)$, wo $f_i(x)\, U_{k'}^i$ in U_k^i liegt; dann gehört xV_{l_m} zu V_m. Bedeutet V_m aber einen endlichen Durchschnitt von Mengen $f_i^{(-1)}(U_k^i)$, so verwenden wir den Durchschnitt der V_{l_m} entsprechenden Nullumgebungen. (1) vervollständigt den Beweis.

Der Begriff der lineartopologischen Algebra bleibt bei den üblichen topologischen Operationen erhalten:

(8) *Sei S eine Subalgebra einer lineartopologischen Algebra $L(T)$; dann ist S in bezug auf die durch T induzierte Topologie lineartopologisch und die abgeschlossene Hülle $\bar{S}$ von S ist eine Subalgebra. Ebenso ist die abgeschlossene Hülle eines rechten (linken, zweiseitigen) Ideals ein Ideal derselben Art.*

Die erste Behauptung folgt aus (7). Seien nun x_0 und y_0 Elemente aus S. Zu jeder Nullumgebung U_i gibt es dann Elemente x und y aus S, so daß x in $x_0 + U_i$ und y in $y_0 + U_i$ liegen. Wenn $x_0 y_0 + U$ eine Umgebung von $x_0 y_0$ ist, so kann man wegen (3) Nullumgebungen U_l und U_m finden, so daß xy zu $x_0 y_0 + U$ gehört, wenn x und y Elemente von $x_0 + U_l$ bzw. $y_0 + U_m$ sind. Also ist $x_0 y_0$ Berührungspunkt von S. Entsprechend

folgt, daß S abgeschlossen ist bezüglich Addition und skalarer Multiplikation. — Ist H ein Ideal in L, so ist $\overline{Hx}$ enthalten in $\overline{Hx} = \overline{H}$, da eine stetige Abbildung einen Berührungspunkt in einen Berührungspunkt überführt.

(9) *Das topologische Produkt lineartopologischer Algebren ist eine lineartopologische Algebra; dasselbe gilt für die topologische direkte Summe. Dabei sei das Ringprodukt jedesmal komponentenweise erklärt. In beiden Fällen existiert eine Nullumgebungsbasis aus Idealen, wenn dies für die Faktoren bzw. Summanden richtig ist.*

Die erste Aussage ist ein Sonderfall von Satz 2. Auch für die topologische direkte Summe, für welche als Nullumgebungen die direkten Summen von Nullumgebungen der einzelnen Summanden genommen werden, ist die Behauptung klar.

Nimmt man den Grundkörper K selbst als Faktor, so erhält man die lineartopologischen Algebren $\omega_d(K) = \omega_d$ und $\varphi_d(K) = \varphi_d$: Die Algebra ω_d ist das topologische Produkt, φ_d die topologische direkte Summe einer Menge der Mächtigkeit d lineartopologischer Algebren K. Man erkennt, daß die Topologie von φ_d die diskrete ist.

(10) *Wenn $L(T)$ eine lineartopologische Algebra ist und H ein abgeschlossenes, zweiseitiges Ideal in L, so ist die Algebra L/H bezüglich der induzierten Topologie lineartopologisch. L/H ist idealtopologisch, falls L es ist.*

Dies ist leicht zu sehen. Wegen (2) sind die offenen Mengen in L/H gerade die Bilder der offenen Mengen von L bei der Abbildung von L auf L/H. Die Abgeschlossenheit von H garantiert, daß die bei dieser Abbildung übertragene lineare Topologie separiert ist (vgl. [VIII], § 4, 7).

Wir können eine lineartopologische Algebra $L(T)$ in eine lineartopologische Algebra L^+ mit Einselement einbetten: Auf $L \times K$ definieren wir

$$(x, r) + (y, s) = (x + y, r + s); \; r(x, s) = (rx, rs);$$
$$(x, r)(y, s) = (xy + ry + sx, rs).$$

Verwenden wir in der so erhaltenen Algebra mit Einselement $(o, 1)$ die Produkttopologie, so ist L^+ ein lineartopologischer Raum, und eine Nullumgebungsbasis ist in allen Mengen $V_i = (U_i, 0)$ gegeben. Diese Mengen sind Subalgebren; sie sind zweiseitige Ideale in L^+, wenn die Nullumgebungen U_i von L zweiseitige Ideale dieser Algebra sind. Außerdem ist, wovon man sich leicht überzeugt, die Ringmultiplikation stetig. Also haben wir:

(11) *Ist $L(T)$ eine lineartopologische Algebra, so ist L^+ ebenfalls lineartopologisch. L^+ hat eine Nullumgebungsbasis aus zweiseitigen Idealen, wenn L eine solche besitzt.*

(12) *Sei (U_i) eine Nullumgebungsbasis aus zweiseitigen Idealen der idealtopologischen Algebra $L(T)$; dann ist die vollständige Hülle $\overline{L}$ von L auch eine idealtopologische Algebra und sie besitzt eine Nullumgebungsbasis in den zweiseitigen Idealen $\overline{U}_i$, wo $\overline{U}_i$ die abgeschlossene Hülle von U_i in $\overline{L}$ sei. Es ist $U_i = \overline{U}_i \cap L$.*

Beweis. Nach [VIII], § 7, ist $\overline{L}$ ein lineartopologischer Raum mit einer Nullumgebungsbasis $(\overline{U}_i)$; wegen der Abgeschlossenheit der Mengen U_i in L ist $U_i = \overline{U}_i \cap L$. Als Folge von [I], chap. II, § 3, théorème 1, und Satz 1 kann das Ringprodukt gleichmäßig stetig (bezüglich beider Faktoren) auf ganz $\overline{L}$ fortgesetzt werden. Die Gültigkeit der algebraischen Rechenregeln folgt aus der Stetigkeit der Operationen und daraus, daß L in $\overline{L}$ dicht ist. Seien nun x in $\overline{U}_i$ und y in $\overline{L}$ gelegen; wegen der Stetigkeit des Ringproduktes gibt es zu jeder Umgebung U von xy in $\overline{L}$ Umgebungen U_x und U_y von x bzw. y in L mit $U_x U_y < U$. Die Umgebung U_x enthält ein Element u aus U_i und U_y ein Element v

aus L, also liegt das Element uv aus U_i in U, und xy gehört demnach zu $\overline{U}_i$; d. h. $\overline{U}_i$ ist ein zweiseitiges Ideal in $\overline{L}$.

Mit Jacobson führen wir die folgenden Bezeichnungen ein: x heißt *rechts quasiregulär* in L, wenn es ein Element x' in L gibt, so daß $x \circ x' = x + x' + xx' = o$ ist; man nennt x' dann eine *rechte Quasiinverse* von x; entsprechend für *links quasiregulär*; x heißt *quasiregulär*, wenn es links und rechts quasiregulär ist. Es gilt

$$x \circ (y \circ z) = (x \circ y) \circ z .$$

Ist x quasiregulär, so ist jede rechte Quasiinverse x' zugleich linke Quasiinverse und eindeutig bestimmt, denn es ist für eine linke Quasiinverse x''

$$x'' = x'' \circ (x \circ x') = (x'' \circ x) \circ x' = x' .$$

Ein (rechtes, linkes) zweiseitiges Ideal heißt quasiregulär, wenn es nur (rechts, links) quasireguläre Elemente enthält. Die Vereinigung der quasiregulären rechten Ideale von L nennt man das *Radikal* R von L. Die Algebra L ist *halbeinfach*, wenn $R = o$ ist; L heißt eine *Radikalalgebra* für $R = L$. Der Skalar $r \neq 0$ aus K gehöre genau dann zum *Spektrum* eines Elementes x von L, wenn $-\frac{1}{r}x$ nicht rechts quasiregulär ist; $r = 0$ zählt dann und nur dann zum Spektrum, wenn x nicht regulär ist, d. h. kein inverses Element besitzt (in einer Algebra ohne Einselement gehört also 0 zum Spektrum jedes Elementes).

Wir formulieren einige Bemerkungen über das Radikal und die Quasiregularität, welche wir im folgenden benötigen.

(13) *Das Radikal R von L ist ein zweiseitiges Ideal und jedes Element aus R ist quasiregulär in R* (vgl. [V], theorem 1).

(14) *Sei das Radikal einer lineartopologischen Algebra $L(T)$ abgeschlossen; dann ist die lineartopologische Algebra L/R halbeinfach.*

Beweis. Liege das Bild $\hat{x}$ eines Elementes x aus L im Radikal von L/R, d. h. es sei $r\hat{x} + \hat{x}\hat{y}$ rechts quasiregulär für alle $r \in K$ und $y \in L$. Es gibt also ein Element z in L, so daß $(rx + xy) \circ z$ in R liegt, d. h. ein Element u aus L erfüllt die Gleichung $(rx + xy) \circ (z \circ u) = o$, woraus $x \in R$ und $\hat{x} = o$ folgt.

Es gilt ferner:

(15) *In einer idealtopologischen Algebra $L(T)$ mit Radikal R und vollständiger Hülle $\overline{L}$ ist die Quasiinversion gleichmäßig stetig und die abgeschlossene Hülle $\overline{R}^{\overline{L}}$ von R in $\overline{L}$ ist enthalten im Radikal $R(\overline{L})$ von $\overline{L}$.*

Beweis (vgl. [VII], lemma 1). Seien x' und y' die Quasiinversen von x bzw. y; dann liegt

$$x' - y' = \{(y - x) + x'(y - x)\} + \{(y - x) + x'(y - x)\}\, y'$$

in dem offenen Ideal U_i, wenn $y - x$ zu U_i gehört; das beweist die gleichmäßige Stetigkeit der Quasiinversion. Konvergiert das Cauchysystem x^i, wo $x^i \in R$, gegen das Element x von $\overline{R}^{\overline{L}}$, so bilden demnach die Quasiinversen $x^{i\prime}$ ein Cauchysystem in L, d. h. sie konvergieren gegen ein Element x' aus $\overline{L}$; weil $x^i \circ x^{i\prime} = o$ gegen $x \circ x'$ konvergiert, ist x quasiregulär. Nun ist $\overline{R}^{\overline{L}}$ nach der Schlußweise von (12) ein zweiseitiges Ideal in $\overline{L}$, welches also nur quasireguläre Elemente enthält; daraus folgt die Behauptung.

In Analogie zu (14) erhalten wir dann:

(16) *Ist $L(T)$ eine idealtopologische Algebra und ist $\overline{R}^L$ gleich $R(\overline{L})$, so ist $L/\overline{R}^L$ halbeinfach, wo $\overline{R}^L$ die abgeschlossene Hülle von R in L bedeutet.*

Beweis. Liege $\hat{x}$ im Radikal von $L/\overline{R}^L$; dann gibt es für jedes $r \in K$ und $y \in L$ ein Element z in L, so daß $(rx + xy) \circ z$ zu $\overline{R}^L < R(\overline{L})$ gehört. Alle Elemente $a = rx + xy$ haben also Quasiinversen $a' = z \circ u$ in $\overline{L}$, wo u die Quasiinverse von $(rx + xy) \circ z$ ist. Wenn $y \in \overline{L}$ ist, existiert ein gegen y konvergentes Cauchysystem y^i in L, so daß $rx + xy^i$ gegen $rx + xy$ konvergiert; wegen (15) bilden die Elemente $a^{i\prime} = (rx + xy^i)'$ ein Cauchysystem in $\overline{L}$, welches gegen die Quasiinverse a' von $rx + xy$ konvergiert. Also liegt x in $R(\overline{L}) = \overline{R}^{\overline{L}}$, d. h. x ist enthalten in $\overline{R}^{\overline{L}} \frown L = \overline{R}^L$ und folglich ist $\hat{x} = o$.

Gibt es in einer Menge M von rechten Idealen der Algebra L stets ein Ideal V, das in allen Idealen von M enthalten ist, so sagen wir, L genüge der Minimumbedingung für rechte Ideale.

(17) *Genügt eine lineartopologische Algebra der Minimumbedingung für rechte Ideale, so ist $R^n = o$ für ein passendes ganzzahliges n.*

Beweis. Wir folgen [IV], theorem 22. 13. 5. Es sind $R, (R^2), \cdots$ zweiseitige Ideale und es gilt $R > (R^2) > \cdots$. Nach Voraussetzung wird einmal $(R^n) = (R^{n+1})$; setzen wir $(R^n) = S$, so ist $(S^2) = S$ wegen $(R^n) = (R^{2n}) < ((R^n)^2)$ und $(R^n)^2 < (R^{2n})$. Wenn $S \neq o$ ist, gibt es in L ein kleinstes rechtes Ideal H, welches in S enthalten ist und für das $HS \neq o$ ist (S selbst ist ein solches Ideal). Sei $b \in H$ und $bS \neq o$; dann ist das rechte Ideal bS von L enthalten in H, also $bS = H$; insbesondere existiert ein Element z in S mit $bz = -b$. Als Element von R hat z eine rechte Quasiinverse u, d. h. es ist $bz + bu + bzu = o$, also $bz = -b = o$ entgegen Konstruktion. Folglich ist $S = o$.

(18) *Das Radikal einer Algebra enthält den Durchschnitt der maximalen rechten Ideale.*

Der Beweis in [IV], theorem 22. 15. 1 und corollary 3, läßt sich ebenso bei unserer Definition des Radikals führen.

(19) *$R \times 0$ ist das Radikal von L^+, wenn R das Radikal von L ist.*

Denn für das Element (x, r) aus L^+ mit $r \neq 0$ ist $-\frac{1}{r}(x, r)$ nicht rechts quasiregulär, da

$$-\frac{1}{r}(x, r) + (y, s) - \frac{1}{r}(x, r)(y, s) = (o, 0)$$

den Widerspruch

$$-1 + s - s = 0$$

nach sich zieht. Außerdem ist $L \times 0$ ein zweiseitiges Ideal in $L \times K$ und es hat also ein Element $(x, 0)$ eine rechte Quasiinverse schon in $L \times 0$, wenn es sie in $L \times K$ hat.

(20) *Das Radikal $R(H)$ eines zweiseitigen Ideals H von L ist gleich dem Durchschnitt des Radikals R von L mit H.*

In Analogie zu dem Beweis von [VII], lemma 2, schließen wir folgendermaßen: Gewiß ist $R \frown H$ in $R(H)$ enthalten, denn mit einem Element v ist auch seine Quasiinverse $v' = -v - vv'$ in H gelegen. Liegt umgekehrt das Element x in $R(H)$, so auch

das Element $-r^2xx - rxxy - rxyx - xyxy$ für beliebigen Skalar $r \in K$ und $y \in L$. Sei z' die Quasiinverse dieses Elementes. Man rechnet leicht nach, daß

$$(rx + xy) \circ ((-rx - xy) \circ z') = o$$

ist, d. h. es gehört x zum Radikal von L.

Sei $L(T)$ eine idealtopologische Algebra und (U_i), mit $i \in I$, eine Nullumgebungsbasis aus zweiseitigen Idealen; für ein Element x aus L bedeute $p_i(x) = x_i$ das Bild in $L_i = L/U_i$. Unter gewissen Einschränkungen bedingen Quasiregularität von x und von allen x_i sich gegenseitig.

Definition. Wir nennen das linke (rechte) Ideal H einer Algebra L *regulär*, wenn es in L ein Element z gibt, so daß $x - xz$ (bzw. $x - zx$) in H liegt für alle $x \in L$. Das Element z heißt eine *rechte* (bzw. *linke*) *Einheit* modulo H.

Damit gilt zunächst:

(21) *Genau dann ist x_i quasiregulär in L_i für alle i, wenn $-x$ keine Einheit modulo einem eigentlichen, abgeschlossenen, regulären, einseitigen Ideal von L ist.*

Beweis. Wenn x_i etwa keine linke Quasiinverse in L_i hat, so ist $(y + yx_i)$, wo y in L_i läuft, ein abgeschlossenes, eigentliches, reguläres, linkes Ideal G; denn es enthält das Element $-x_i$ nicht. $p_i^{(-1)}(G)$ ist ersichtlich ein eigentliches, reguläres, linkes Ideal mit rechter Einheit $-x$ in L; das Ideal $p_i^{(-)}(G)$ ist wegen der Stetigkeit der kanonischen Abbildung p_i abgeschlossen in L. — Ist andererseits $-x$ eine rechte Einheit modulo einem eigentlichen, abgeschlossenen, regulären, linken Ideal H von L, so gibt es einen Index i, so daß $p_i(H) \neq L_i$ ist; denn es existiert ein Element v in L und ein U_i mit $(v + U_i) \cap H = \emptyset$, d. h. es ist $p_i(v)$ nicht in $p_i(H)$ gelegen. — x_i ist rechte Einheit modulo $p_i(H)$ und $p_i(H)$ enthält das Ideal $(y + yx_i)$, wo y die Algebra L_i durchläuft. Aus der Annahme, x_i sei links quasiregulär in L_i, erhalten wir dann den Widerspruch $(y + yx_i) = L_i$: Sei $z \in L_i$ eine linke Quasiinverse von x_i; es folgt $x_i \in (y + yx_i)$ und also $y \in (y + yx_i)$ für alle y aus L_i, denn es ist $x_i = -z - zx_i$. Hiermit folgt:

(22) *Wenn in einer idealtopologischen Algebra $L(T)$ jedes reguläre, maximale Ideal abgeschlossen ist, so ist ein Element x aus L genau dann quasiregulär in L, wenn x_i quasiregulär ist in L_i für alle i.*

Beweis. Die Notwendigkeit trifft zu, weil Quasiregularität bei homomorpher Abbildung p_i erhalten bleibt; denn ist x' die Quasiinverse von x, so hat $p_i(x)$ die Quasiinverse $p_i(x')$, wie durch Anwendung von p_i auf $x + x' + xx' = o$ folgt. — Hat das Element x aus L etwa keine linke Quasiinverse, so ist das reguläre linke Ideal $(y + yx)$, wo y in L läuft, wie unter (21) eigentlich und es kann wie in [IV], theorem 22. 14. 3, in ein reguläres, maximales linkes Ideal H mit derselben rechten Einheit $-x$ eingebettet werden. Da H nach Voraussetzung abgeschlossen ist, können wir (21) anwenden.

In solchen Algebren ist das Radikal abgeschlossen:

(23) *Sei ein Element x einer idealtopologischen Algebra $L(T)$ rechts quasiregulär in L, wenn x_i quasiregulär ist in L_i für alle i; dann ist das Radikal R von L abgeschlossen.*

Beweis. R_i bezeichne das Radikal von L_i. Weil Quasiregularität bei homomorpher Abbildung erhalten bleibt, ist R enthalten in $D = \bigcap_{i \in I} p_i^{(-1)}(R_i)$. Der Durchschnitt D ist ein abgeschlossenes (L_i ist diskret), zweiseitiges Ideal in $L(T)$ und jedes Element von D ist nach Voraussetzung rechts quasiregulär, also liegt D in R.

Eine lineartopologische Algebra, welche aus $\varphi_{\aleph_0} = \varphi$ und $\omega_{\aleph_0} = \omega$ durch eine wohlgeordnete Folge, bis zur 2. Zahlklasse, von topologischen Summen- und Produktbildungen entsteht, heiße eine *Algebra abzählbarer Stufe.*

(24) *Das Spektrum eines Elementes x aus φ_d, ω_d oder einer Algebra abzählbarer Stufe besteht genau aus allen Skalaren r, welche als Komponenten von x auftreten; es ist deshalb endlich für $x \in \varphi_d$ und höchstens abzählbar, wenn x in einer Algebra abzählbarer Stufe liegt. x ist also quasiregulär, wenn keine Komponente gleich -1 ist.*

Beweis. Die Gleichung $s + t + st = 0$ ist genau für $t \neq -1$ lösbar. Indem man sie komponentenweise für $-\frac{1}{r}x$ löst, wo r unter den Komponenten von x nicht vorkomme, erhält man ersichtlich eine Quasiinverse von $-\frac{1}{r}x$ in L, denn $t = 0$ hat $s = 0$ zur Folge und L enthält zu einem Element y alle „Vektoren" mit gleichen Nullkomponenten. Hat andererseits ein Element y aus L die Komponente -1, so kann es nach unserer Überlegung keine Quasiinverse haben, d. h. auch nur dann besitzt $-\frac{1}{r}x$ eine Quasiinverse, wenn r unter den Komponenten von x nicht auftritt. Auch hat x offenbar genau dann eine Nullkomponente, wenn x nicht regulär ist in L.

Die folgenden Überlegungen versuchen eine Charakterisierung lineartopologischer Räume bzw. Algebren.

(25) *Auf einem linearen Raum L sei eine separierte Topologie T erklärt. Der topologische Raum $L(T)$ ist genau dann lineartopologisch, wenn er topologisch isomorph ist zu einem Teilraum S des topologischen Produktes diskreter, linearer Räume. Ein entsprechender Satz gilt für idealtopologische Algebren.*

Beweis. Sei (U_i), mit $i \in I$, eine Nullumgebungssubbasis aus linearen Teilräumen von $L(T)$. Die Zuordnung $x \to (x_i)$, wo x_i die Restklasse $x + U_i$ bedeutet, gibt uns eine topologisch isomorphe Abbildung von $L(T)$ in das topologische Produkt der diskreten Räume L/U_i. — Wenn L eine Algebra mit einer Nullumgebungsbasis (U_i) aus zweiseitigen Idealen ist, so ist obige Zuordnung ein Homomorphismus, und das topologische Produkt ist ebenfalls idealtopologisch. Umgekehrt ist ein topologisches Produkt diskreter Algebren, wie man sofort sieht, eine idealtopologische Algebra, also auch jede Subalgebra.

Im Fall einer vollständigen idealtopologischen Algebra können wir die Subalgebra S genauer bestimmen:

Satz 3. *Eine vollständige lineartopologische Algebra mit einer Nullumgebungsbasis aus zweiseitigen Idealen U_i ist der projektive Limes der idealtopologischen Algebren L_i.*

Beweis. Wir setzen $i \leqq j$ für $U_j < U_i$ und machen so die Indizesmenge I zu einem gerichteten System. Aus $x_j = y_j$ folgt dann $x_i = y_i$, so daß durch

$$f_{ij}(x_j) = x_i \text{ für } i \leqq j$$

eine topologisch homomorphe Abbildung von L_j auf L_i erklärt ist; sie genügt der Gleichung

$$f_{ik}(x_k) = f_{ij}(f_{jk}(x_k)) \text{ für } i \leqq j \leqq k,$$

denn beide Seiten bedeuten die Restklasse von x modulo U_i. Im topologischen Produkt P der Algebren L_i betrachten wir die Gesamtheit $\lim L_i$ der Elemente x mit

$$p_i(x) = f_{ij}(p_j(x)) \text{ für } i \leqq j.$$

Zunächst ist $S < \lim L_i$. Da es zu je endlich vielen Indizes $i_1, \ldots, i_n$ des gerichteten Systems I stets eine obere Schranke i_m gibt, so ist nach Definition von $\lim L_i$ in der (beliebigen) Umgebung $U = (y \text{ aus } \lim L_i : y_{i_\nu} = x_{i_\nu}, \nu = 1, \ldots, n)$ einer Umgebungsbasis des Elementes x aus $\lim L_i$ die durch eine einzige Bedingung gekennzeichnete

Umgebung $V = (y \text{ aus } \lim L_i : y_{i_m} = x_{i_m})$ enthalten; dabei wird $\lim L_i$ als Teilraum von P betrachtet. Es gibt ein Element z aus S mit $z_{i_m} = x_{i_m}$, d. h. z liegt in U. Also ist S dicht in $\lim L_i$ und folglich gleich $\lim L_i$, weil S nach Voraussetzung abgeschlossen ist in P, d. h. auch in $\lim L_i$.

Diese Kennzeichnung von S ergibt:

(26) *Die vollständige idealtopologische Algebra $L(T)$ hat genau dann ein Einselement, wenn jede Algebra L_i ein Einselement besitzt. Außerdem ist ein Element x aus L genau dann regulär oder quasiregulär in L, wenn x_i es ist in L_i für alle $i \in I$.*

Beweis. Daß die Bedingungen notwendig sind, ist klar. Sei e_i das Einselement von L_i, für $i \in I$. Wenn $i \leqq j$ ist, so haben wir

$$f_{ij}(e_j)\, x_i = f_{ij}(e_j x_j) = x_i \text{ für alle } i,$$

d. h. es gilt

$$e_i = f_{ij}(e_j),$$

und das Element e aus P mit den Komponenten e_i liegt nach obigem in S. Da $(ex)_i = e_i x_i = x_i$, d. h. $(ex - x)_i = o$ ist für alle i, gilt $ex = x$. — Ist x_i' die Quasiinverse von x_i für alle i, so erhalten wir

$$f_{ij}(x_j') \circ x_i = f_{ij}(x_j' \circ x_j) = o,$$

also

$$x_i' = f_{ij}(x_j'), \text{ wenn } i \leqq j \text{ ist.}$$

Wie eben liegt das Element x' mit den Komponenten x_i' in S und x_i' ist die Quasiinverse von x in L. — Für den regulären Fall verläuft der Nachweis ebenso.

Nach (21) gilt:

(27) *Das Element x einer vollständigen idealtopologischen Algebra $L(T)$ ist genau dann quasiregulär, wenn $-x$ keine Einheit modulo einem eigentlichen, abgeschlossenen, einseitigen, regulären Ideal in L ist.*

Eine Anwendung auf das Radikal ergibt mit (23):

Satz 4. *Das Radikal einer vollständigen idealtopologischen Algebra ist abgeschlossen.*

Dies läßt sich auch aus der gleichmäßigen Stetigkeit der Quasiinversion schließen (vgl. (15)). Außerdem kann man eine lineartopologische Algebra als Teil einer Transformationsalgebra beschreiben.

Die Gesamtheit $S(L)$ der stetigen Endomorphismen eines lineartopologischen Raumes $L(T)$ bildet ersichtlich eine Algebra, wenn man das Produkt AB zweier Endomorphismen A und B durch $AB(x) = A(B(x))$ erklärt. Es gilt:

Satz 5. *Versieht man $S(L)$ mit der Topologie T_u der uniformen Konvergenz in L (vgl. [II], § 1), so wird $S(L)$ eine lineartopologische Algebra mit einer Nullumgebungsbasis aus rechten Idealen.*

Beweis. (U_i), mit $i \in I$, gebe eine Nullumgebungsbasis aus linearen Teilräumen von L an. H_i bezeichne die Menge aller Abbildungen $A \in S(L)$, welche L abbilden in U_i; diese Mengen sind nichtleer und rechte Ideale in $S(L)$; sie bilden eine Nullumgebungsbasis für T_u. Liegt der Endomorphismus A in allen H_i, so ist A offenbar die Nullabbildung o. Eine Umgebungsbasis von $A_0 \neq o$ ist in T_u gegeben durch Mengen G_i aller Elemente A aus $S(L)$, für welche $A(x) - A_0(x)$ stets in U_i liegt, wenn x ein beliebiges Element aus L ist. Das Element $A - A_0$ aus $S(L)$ liegt also in H_i, d. h. jedes Element aus G_i stammt aus $A_0 + H_i$; umgekehrt gehört auch jedes Element A von $A_0 + H_i$

zu G_i. Die Topologie T_u ist also linear und $S(L)$ (T_u) ist nach (7) ein lineartopologischer Raum. Um die Stetigkeit des Produktes AB nachzuweisen, genügt es im Fall der Rechtsmultiplikation bei gegebener Nullumgebung H_i diese selbst zu wählen, denn es ist $H_i B < H_i$; andererseits gibt es zu einem stetigen Endomorphismus A eine Nullumgebung U_k von L, so daß $A(U_k)$ in U_i liegt; für die Linksmultiplikation kann man also H_k nehmen, AH_k liegt in H_i. Nach (1) genügt dieser Nachweis der Stetigkeit in o.

Umgekehrt erhalten wir:

Satz 6. *Zu jeder lineartopologischen Algebra $L(T)$ mit einer Nullumgebungsbasis (U_i) aus rechten Idealen gibt es einen lineartopologischen Raum E, so daß L topologisch isomorph ist zu einer Subalgebra von $S(E)$ mit der Topologie der uniformen Konvergenz in E. Hat L ein Einselement, so kann man $E = L$ wählen, sonst $E = L^+$.*

Beweis. Die Multiplikation aller Elemente y aus L mit x von links her ist eine lineare Abbildung A_x, welche wegen der Stetigkeit von xy zu $S(L)$ gehört. Besitzt L ein Einselement e, so ist die Zuordnung zwischen x und A_x eineindeutig; sie ist eine algebraische Isomorphie mit dem Produkt aus Satz 5. Wenn x in U_i liegt, so ist $A_x \in H_i$ und umgekehrt, die Isomorphie ist also topologisch. Hat L kein Einselement, so schließen wir ebenso in L^+ statt L. In L^+ ist x das Element $(x, 0)$. Die wie eben erklärte Zuordnung zwischen x bzw. $(x, 0)$ und einem Element A_x aus $S(L^+)$ ist wieder wegen der Existenz eines Einselementes eine algebraische Isomorphie. Wenn x in U_i liegt, so ist

$$(x, 0)\,(y, r) = (xy + rx, 0)$$

ein Element von $V_i = (U_i, 0)$, d. h. A_x gehört zu H_i. Liegt umgekehrt A_x in H_i, so bedeutet dies, daß $A_x((y, r))$ in $(U_i, 0)$ liegt für alle Elemente (y, r) aus L^+; insbesondere ist $(x, 0)\,(r, 1) = (x, 0)$ ein Element von V_i, d. h. x gehört zu U_i. Hiernach wird auch die Topologie bei der Isomorphie übertragen, sie ist also eine Homöomorphie. — Natürlich kann man den Satz auch für linke Ideale U_i statt rechte formulieren, wenn man im Beweis die Rechtsmultiplikation verwendet und die Produktdefinition für $S(L)$ entsprechend modifiziert.

Wir können das folgende allgemeine Beispiel einer lineartopologischen Algebra anschließen.

Satz 7. *L sei eine Algebra stetiger Funktionen von einem topologischen Raum E in eine lineartopologische Algebra F; das Produkt sei in L durch $fg(x) = f(x)\,g(x)$ für $x \in E$ erklärt. Sei ferner $V = (V_i)$, mit $i \in I$, eine Menge von kompakten Teilmengen von E, deren Vereinigung gleich E ist. Versieht man L mit der Topologie T_v der uniformen Konvergenz in den Mengen V_i, so ist $L(T_v)$ eine lineartopologische Algebra. Ist F eine idealtopologische Algebra, so auch $L(T_v)$.*

Beweis. (U_j), mit $j \in J$, sei eine lineare Nullumgebungsbasis von F. Man kann voraussetzen, daß V jede endliche Vereinigung von Mengen V_i enthält, das ändert die Topologie T_v nicht. Eine Nullumgebungsbasis von L bezüglich T_v besteht damit in den linearen Mengen $H_{ij} = (f$ aus L; $f(x) \in U_j$ für alle $x \in V_i)$, mit $i \in I$ und $j \in J$. Wie in Satz 5 ergibt sich, daß $L(T_v)$ ein lineartopologischer Raum ist. Die Mengen H_{ij} sind Subalgebren von L, denn wenn f und g zu H_{ij} gehören, so ist $fg(x) = f(x)\,g(x) \in U_j$ für alle $x \in V_i$, weil U_j eine Algebra ist. Sind die Nullumgebungen U_j zweiseitige Ideale in F, so werden die H_{ij} zweiseitige Ideale in L. Nun müssen wir zu einem Element f und einer Nullumgebung H_{ij} in L eine zweite Nullumgebung H_{kl} finden, so daß $fH_{kl} < H_{ij}$. Zu $f(x)$, wo x in V_i liegt, gibt es eine offene Umgebung U_x und eine Nullumgebung U_x^* (dies sei ein U_j) mit $U_x U_x^* < U_j$, wegen der Stetigkeit des Ringproduktes bezüglich beider Faktoren

(hier $f(x)$ und o) in F. Die Mengen U_x ergeben eine offene Überdeckung der kompakten Menge $f(V_i)$, wenn x in V_i variiert. Sei $U_{x_1}, \ldots, U_{x_n}$ eine endliche Überdeckung hieraus und die lineare Nullumgebung U_p sei enthalten in $U^*_{x_1} \cap \cdots \cap U^*_{x_n}$. Dann ist $fH_{ip} \subset H_{ij}$, womit die einseitige Stetigkeit des Ringproduktes nachgewiesen ist; denn der Fall der Rechtsmultiplikation erledigt sich wegen der Symmetrie des Produktes fg ganz entsprechend.

Der Beweis enthält die Aussage:

Korollar. *Sei L ein linearer Raum beliebiger Abbildungen einer Menge E in einen lineartopologischen Raum F; bezeichne $V = (V_i)$, mit $i \in I$, eine Klasse von Teilräumen von E, deren Vereinigung gleich E ist. Versieht man L mit der Topologie T_v der uniformen Konvergenz in den Mengen V_i, so ist $L(T_v)$ ein lineartopologischer Raum.*

§ 2. Linear kompakte Algebren und die schwache Topologie. Lokal linear kompakte Algebren.

Ein lineartopologischer Raum $L(T)$ heißt *linear kompakt*, wenn jeder „lineare Filter" d. h. Filter mit einer Basis $(x_i + F_i)$ aus linearen Teilmannigfaltigkeiten $x_i + F_i$ von L, einen Berührungspunkt in L besitzt. Ist eine lineartopologische Algebra als Raum linear kompakt, so heißt sie eine *linear kompakte Algebra.*

Wesentliche Eigenschaften des Begriffes „kompakt" gelten sinngemäß auch für „linear kompakt", wie wir gleich sehen werden. Hingegen folgt aus „$L(T)$ ist linear kompakt" nicht, daß jede Überdeckung von L durch offene lineare Mannigfaltigkeiten eine endliche solche Überdeckung enthält; ein Gegenbeispiel findet sich leicht.

(1) *Ein abgeschlossener linearer Teilraum S eines linear kompakten Raumes ist linear kompakt.*

Dies ist unmittelbar einzusehen.

(2) *Ist A eine lineare stetige Abbildung eines linear kompakten Raumes $L(T)$ in einen lineartopologischen Raum, so ist $A(L)$ linear kompakt. Also ist die Restklassenalgebra L/S der linear kompakten Algebra L nach einem abgeschlossenen, zweiseitigen Ideal S linear kompakt.*

Weil $A^{(-1)}$ einen linearen Filter F auf $A(L)$ in einen ebensolchen auf L überführt, gilt die Behauptung; denn die stetige Abbildung A führt einen Berührungspunkt von $A^{(-1)}(F)$ in L in einen Berührungspunkt von F in $A(L)$ über.

(3) *Wenn jede Hyperebene eines linear kompakten Raumes $L(T)$ abgeschlossen ist (z. B. $L(T)$ diskret), dann ist er endlichdimensional.*

Es gilt der Beweis von [X], II, 6. (27. 7).

Auch die Umkehrung ist richtig:

(4) *Jeder endlichdimensionale lineartopologische Raum ist linear kompakt.*

Zum Beweis vgl. ebenfalls [X], II, 6. (27. 7).

(5) *Ein linear kompakter Raum ist vollständig* (siehe [III], 1. h).

(6) *Das topologische Produkt beliebig vieler linear kompakter Räume ist linear kompakt.*

Beweis wie beim Satz von Tychonoff; vgl. [X], II, 6. (27. 2).

Also ist ω_d mit (4) linear kompakt.

Nach [VIII], § 4, 9, ist eine stetige lineare Abbildung eines linear kompakten Raumes in einen lineartopologischen Raum ein topologischer Homomorphismus. Wenden wir diesen Satz auf die identische Abbildung an, so ergibt sich:

(7) *Wenn ein linear kompakter Raum $L(T)$ bezüglich einer gröberen Topologie T' lineartopologisch ist, so stimmen die beiden Topologien überein. Insbesondere stimmen zwei vergleichbare Topologien, welche beide L zu einem linear kompakten Raum machen, überein.*

Die Topologie eines linear kompakten Raumes $L(T)$ läßt sich mit Hilfe des linearen Raumes L' aller stetigen linearen Abbildungen von L in K beschreiben. Ein Element x aus L und u aus dem *zu $L(T)$ dualen Raum L'* heißen *orthogonal*, wenn $u(x) = 0$ ist. Die *Orthogonalräume* $S^{\perp}$ der endlichdimensionalen linearen Teilräume S von L erklären auf L' eine Topologie (Topologie der einfachen Konvergenz), welche die *schwache Topologie* $T_s(L)$ von L' heißt; entsprechend ist $T_s(L')$ auf L erklärt. Für diese Topologie gilt:

(8) *Eine Nullumgebungsbasis von $T_s(L')$ besteht aus der Gesamtheit der T-abgeschlossenen linearen Teilräume endlichen Defektes von $L(T)$.*

Der *Defekt* eines Teilraumes S eines linearen Raumes L ist erklärt als die Dimension des linearen Raumes L/S.

(9) *Die schwache Topologie $T_s(L)$ ist stets gröber als die ursprüngliche Topologie T.*

(10) *Die lineartopologischen Räume $L(T_s(L'))$ und $L'(T_s(L))$ sind wechselseitig dual zueinander.*

Für die Beweise siehe [VIII], § 4, 4.

(8), (9) und § 1, (2) liefern:

(11) *In einem lineartopologischen Raum $L(T)$ mit einer Nullumgebungsbasis (oder Nullumgebungssubbasis) aus linearen Teilräumen von endlichem Defekt ist $T = T_s$.*

Nun hat wegen (3) und (2) jede lineare Nullumgebung eines linear kompakten Raumes endlichen Defekt, d. h. wir erhalten die angekündigte Kennzeichnung: Auf einem linear kompakten Raum $L(T)$ ist die Topologie T stets die schwache Topologie $T_s(L')$.

Ein lineartopologischer Raum $L(T)$ ist lineartopologisch auch bezüglich der Topologie $T_s(L')$ (vgl. [VIII], § 4). Wir werden sehen, daß dies für eine lineartopologische Algebra $L(T)$ nicht immer richtig ist. Ist eine lineartopologische Algebra $L(T)$ mit der schwachen Topologie eine lineartopologische Algebra $L(T_s)$, so sagen wir „*$L(T)$ läßt T_s zu*"; z. B. läßt eine linear kompakte Algebra T_s zu. Richten wir unser Augenmerk auf lineartopologische Algebren, welche T_s zulassen, so ergibt sich:

Satz 1. *Wenn die lineartopologische Algebra $L(T)$ die Topologie T_s zuläßt, so hat $L(T_s)$ eine Nullumgebungsbasis aus zweiseitigen Idealen mit endlichem Defekt.*

Beweis. Sei U eine schwache lineare Nullumgebung; dann gibt es Elemente $x_1, \ldots, x_n$ in L, so daß $L = (x_1) + \cdots + (x_n) + U$ ist. Zu jedem Element x_i existiert wegen der Stetigkeit des Ringproduktes eine Nullumgebung $U_i < U$, so daß $x_i U_i < U$. Wenn die lineare Nullumgebung V in $U_1 \cap \cdots \cap U_n$ enthalten ist, so liegt LV in U; ebenso finden wir eine lineare Nullumgebung W mit $WL < U$ und $W < U$. Nun können wir den Beweis wie in § 1, Satz 1, zu Ende führen.

Korollar 1. *Eine linear kompakte Algebra ohne eigentliches, offenes, zweiseitiges Ideal ist endlichdimensional.*

Dann ist o eine Nullumgebungsbasis von endlichem Defekt.

Korollar 2. *Ein unendlichdimensionaler Schiefkörper über K läßt T_s nicht zu.*

(12) *Enthält die lineartopologische Algebra $L(T)$ ein offenes, linear kompaktes, zweiseitiges Ideal H mit Einselement e, so ist $L(T)$ idealtopologisch.*

Beweis. Der Durchschnitt einer Nullumgebung U von L mit H enthält nach Satz 1 ein in H und damit in L offenes, zweiseitiges Ideal W von H. Dieses Ideal W von H ist auch ein zweiseitiges Ideal von L, da für $x \in L$ und $y \in W$ das Element $xy = (xe)\,y$ in W liegt.

Satz 2. *Ist $L(T_s)$ eine lineartopologische Algebra, so ist sie linear präkompakt.*

Beweis. (U_i) sei eine Nullumgebungsbasis aus zweiseitigen Idealen. Wir gehen zur vollständigen Hülle $\overline{L}$ von $L(T_s)$ über (vgl. § 1, (12)). Ordnet man für ein Element x aus L der Restklasse x_i von x in L/U_i die Restklasse $\overline{x}_i$ von x in $\overline{L}/\overline{U}_i$ zu, so ist diese Zuordnung wegen $U_i = \overline{U}_i \cap L$ eine Isomorphie zwischen L/U_i und der Subalgebra S derjenigen Restklassen aus $\overline{L}/\overline{U}_i$, welche ein Element aus L enthalten; das sind aber alle, da L dicht ist in $\overline{L}$ und $y + \overline{U}_i$ eine Umgebung von y in $\overline{L}$ darstellt (diese Schlußweise entnehme ich [XV], lemma 1). Also ist $S = \overline{L}/\overline{U}_i$ und diese Algebra ist wie L/U_i endlichdimensional, d. h. linear kompakt. Nach § 1, (25) ist $\overline{L}$ topologisch isomorph einem abgeschlossenen Teilraum des topologischen Produktes der Algebren $\overline{L}/\overline{U}_i$; $\overline{L}$ ist also wegen (6) und (1) linear kompakt.

Korollar. *Die linear kompakten Algebren sind genau die bezüglich der schwachen Topologie vollständigen lineartopologischen Algebren.*

(13) *Eine lineartopologische Algebra $L(T)$, welche T_s zuläßt, besitzt offene, maximale zweiseitige und einseitige Ideale mit endlichem Defekt, und der Durchschnitt aller offenen, zweiseitigen Ideale mit endlichem Defekt ist o. Jedes in $L(T)$ abgeschlossene, maximale Ideal hat endlichen Defekt und ist T_s-offen. $L(T)$ besitzt eigentliche, offene, maximale Ideale, wenn L unendlichdimensional ist.*

Beweis. Die erste Aussage ist nach Satz 1 und (9) klar. Der Durchschnitt der in $L(T)$ offenen, zweiseitigen Ideale mit endlichem Defekt ist gleich dem einer Nullumgebungsbasis von $L(T_s)$, ist also o. Ist M ein in $L(T)$ abgeschlossenes, maximales Ideal, so ist M nach [VIII], § 4, 4 (6) auch T_s-abgeschlossen. Wegen § 1, (6) ist M dann T_s-offen und hat also endlichen Defekt. Wenn L unendlichdimensional ist, kann T_s nicht die diskrete Topologie sein; d. h. es gibt in diesem Fall eigentliche, T_s-offene, zweiseitige (und einseitige) Ideale, die man wegen ihres endlichen Defektes in maximale Ideale derselben Art einbetten kann.

Hieraus folgt:

(14) *Eine lineartopologische Algebra $L(T)$, welche T_s zuläßt, und ein endlichdimensionales, maximales Ideal H enthält, ist endlichdimensional.*

Denn H ist abgeschlossen, da die induzierte uniforme Struktur diskret ist. Nach (13) hat H auch endlichen Defekt.

Dem Korollar 2 von Satz 1 stellen wir zur Seite:

Satz 3. *φ_d läßt T_s nicht zu, außer wenn d endlich ist.*

Zum Beweis benötigen wir die folgende Bemerkung:

(15) *In φ_d ist jedes Ideal H gekennzeichnet als Menge aller Elemente x, deren Komponenten $x_{i'}$ verschwinden für $i' \in I'$, wo I' eine gewisse Teilmenge der Komponentenindizesmenge I ist.*

Beweis. e_i bezeichne das Element von φ_d, dessen Komponenten alle gleich 0 sind außer der i-ten, die gleich 1 ist. Wenn für ein Element x aus H die Komponente $x_i = r \neq 0$ ist, so liegt $e_i \frac{1}{r} x = e_i$ in H. Ist demnach $I'' = (i'')$ die Teilmenge von I, für welche ein x in H existiert mit $x_{i''} \neq 0$, so ist H gerade die direkte Summe aller Algebren $Ke_{i''}$, mit $i'' \in I''$, was unsere Behauptung beweist. Man sieht noch, daß genau die Ideale in φ_d regulär sind, welche durch endlich viele Bedingungen $x_{i_1} = 0, \ldots, x_{i_n} = 0$ angegeben werden können.

Nehmen wir nun an, $\varphi_d(T_s)$ sei eine lineartopologische Algebra. Da φ_d diskret ist, gibt es in φ_d' ein Element u, so daß $u(e_i) \neq 0$ ist für unendlich viele $i \in I$. Die T_s-Nullumgebung $u^\perp$ kann dann kein Ideal G mit endlichem Defekt enthalten; denn G wäre nach unserer obigen Überlegung gekennzeichnet durch eine Indizesmenge I', so daß $I - I'$ endlich wäre, und es könnten also im Komplement von G in φ_d nur endlich viele e_i liegen.

Unmittelbar aus § 1, (2), sowie (13) und (9) ergibt sich:

(16) *Die lineartopologische Algebra $L(T)$ lasse T_s zu und besitze eine Nullumgebungssubbasis aus maximalen zweiseitigen Idealen; dann ist T die schwache Topologie.*

In teilweiser Umkehrung gilt:

(17) *Eine halbeinfache, linear kompakte Algebra $L(T)$ besitzt eine Nullumgebungssubbasis aus maximalen zweiseitigen Idealen.*

Beweis. Wir zeigen zunächst, daß der Durchschnitt D der offenen, maximalen zweiseitigen Ideale M von $L(T)$ gleich o ist. Sei (U_i) eine Nullumgebungsbasis von $L(T)$ aus zweiseitigen Idealen. Wenn N ein offenes, maximales rechtes Ideal ist, so enthält N eine Nullumgebung U_j und da L/U_j endlichdimensional ist, liegt eines der Ideale M in N. Ein Element x aus D ist daher auch in allen offenen, maximalen rechten Idealen gelegen; dies gilt dann auch für das Element $rx + xy$ für beliebigen Skalar r und $y \in L$. Das Element $r\hat{x} + \hat{x}\hat{y}$ aus L/U_i liegt also für jedes i in allen maximalen rechten Idealen von L/U_i. Nach § 1, (18) und § 1, (17) gibt es folglich eine ganze Zahl n, so daß $(rx + xy)^n$ in U_i liegt; d. h. die n-ten Potenzen von $z = rx + xy$ konvergieren gegen o. Dann ist die Folge $z_n = -z + z^2 - \cdots + (-1)^n z^n$ eine Cauchyfolge und konvergiert also gegen ein Element z' von L. Weil $z \circ z_n = z(-1)^n z^n$ gegen o und gegen $z \circ z'$ konvergiert für wachsendes n, gilt $z \circ z' = o$. Das Element x erzeugt somit ein quasireguläres, rechtes Ideal in L und ist darum nach Voraussetzung gleich o. — Nehmen wir zu der Menge aller offenen, maximalen zweiseitigen Ideale M von $L(T)$ noch alle endlichen Durchschnitte solcher Ideale hinzu, dann können wir mit der so erhaltenen Filterbasis nach § 1, (7) auf L eine Topologie T' konstruieren, und $L(T')$ ist lineartopologisch; T' ist gröber als T, also ist sie wegen (7) gleich T.

Da in einer linear kompakten Algebra das Radikal R nach § 1, Satz 4, abgeschlossen und darum gemäß § 1, (14) die Restklassenalgebra L/R halbeinfach ist, folgt:

(18) *In einer linear kompakten Algebra ist das Radikal gleich dem Durchschnitt der es enthaltenden offenen, maximalen zweiseitigen Ideale.*

Außerdem gilt:

(19) *Wenn $L(T)$ eine linear kompakte Algebra ist, gibt es zu jeder Nullumgebung U von $L(T)$ eine ganze Zahl n, so daß R^n in U enthalten ist. In einer kommutativen, linear kompakten Algebra ist R die Gesamtheit der Elemente x aus L, deren n-ten Potenzen gegen o konvergieren.*

Beweis. Das Bild $\hat{R}$ von R in L/U ist im Radikal dieser endlichdimensionalen Algebra enthalten; wir konnten dabei annehmen, daß U ein zweiseitiges Ideal ist; die Behauptung folgt dann aus § 1, (17). Insbesondere konvergieren die n-ten Potenzen jedes Elementes x aus R gegen o. Konvergieren andererseits in einer kommutativen linear kompakten Algebra die Elemente x^n und y^n gegen o, so auch rx^n, $(xz)^n$ und $(x+y)^n$. Nach dem Beweis von (17) ergibt sich die zweite Aussage.

Die Ausführungen von § 1, (25) besagen, daß eine linear kompakte Algebra topologisch isomorph ist zu einer Subalgebra des topologischen Produktes endlichdimensionaler Algebren. Im halbeinfachen Fall können wir dieses Ergebnis verfeinern.

Zunächst erhalten wir:

Satz 4. *Eine lineartopologische Algebra $L(T_s)$ besitze eine Nullumgebungssubbasis (U_i), mit $i \in I$, aus maximalen zweiseitigen Idealen U_i; dann ist $L(T_s)$ topologisch isomorph einer dichten Subalgebra S eines topologischen Produktes endlichdimensionaler, einfacher Algebren.*

Beweis. Wir denken uns die Indizesmenge I wohlgeordnet und wählen folgendermaßen eine Teilmenge (V_j), mit $j \in J \subset I$, unter den U_i aus: V_1 sei gleich U_1; wenn V_j für alle $j < k$ bereits ausgewählt ist, so nehmen wir als V_k das erste U_i, welches alle endlichen Durchschnitte irgendwelcher Mengen V_j mit $j < k$ nicht enthält. Die Mengen V_j bilden dann auch eine Nullumgebungssubbasis von $L(T_s)$. Nach § 1, (25) ist $L(T_s)$ topologisch isomorph einer Subalgebra S des topologischen Produktes P der endlichdimensionalen (diskreten) einfachen Algebren $L_j = L/V_j$. Seien nun für $l = 1, \ldots, n$ Elemente x_{j_l} aus L_{j_l} gegeben, $j_1, j_2, \ldots$ wachsend. Um nachzuweisen, daß S dicht ist in P, müssen wir ein Element y in S auffinden mit Komponenten

$$p_j(y) = \begin{cases} x_j \text{ für } j = j_l; \quad l = 1, \ldots, n, \\ \text{beliebig sonst}; \end{cases}$$

p_j bedeute dabei in P die Projektion auf die j-te Komponente. Für alle Indizes $l \leqq n-1$ seien bereits Elemente z^l aus S gefunden, für welche

$$p_{j_m}(z^l) = \begin{cases} o \text{ für } m < l; \quad m \text{ aus } 1, \ldots, n-1 \\ x_{j_l} - \sum\limits_{\lambda=1}^{l-1} p_j(z^\lambda) \text{ für } m = l \end{cases}$$

gilt. Nach unserer Konstruktion der V_j gibt es ein Element z'^n in S, so daß

$$p_{j_m}(z'^n) = \begin{cases} o \text{ für } m < n \\ u \neq o, u \in L_{j_n}, \text{ für } m = n \end{cases}$$

ist. L_{j_n} ist als endlichdimensionale Algebra ohne eigentliches, zweiseitiges Ideal eine volle Matrizenalgebra über einem Schiefkörper K^* über K oder es gilt $L_{j_n}^2 = o$. Im ersten Fall hat L_{j_n} ein Einselement, weshalb $(L_{j_n} u L_{j_n})$ ein nichtverschwindendes, zweiseitiges Ideal in L_{j_n} und damit gleich L_{j_n} ist. Hieraus folgt $p_{j_n}((Lz'^nL)) = L_{j_n}$; alle Elemente von (Lz'^nL) haben Nullkomponenten an den Stellen $j_1, \ldots, j_{n-1}$. Es existiert also ein Element z^n in S mit

$$p_{j_m}(z^n) = \begin{cases} o \text{ für } m < n \\ x_{j_n} - \sum\limits_{\lambda=1}^{n-1} p_{j_n}(z^\lambda) \text{ für } m = n. \end{cases}$$

Im zweiten Fall ist L_{j_n} eindimensional, weil jeder lineare Teilraum ein zweiseitiges Ideal ist. Hier kann für z^n ein skalares Vielfaches von z'^n genommen werden. Bilden wir jetzt $z^1 + \cdots + z^n$, so ist dies das gesuchte Element y aus S; die Subalgebra S ist also dicht in P.

Wir schließen folgende Bemerkung an: Nehmen wir an, es sei $L_j^2 \neq o$ für alle $j \in J$ (z. B. $L_i^2 \neq o$ für alle $i \in I$). Wenn M ein maximales zweiseitiges Ideal in P ist, so ist $p_j(M)$ stets ein zweiseitiges Ideal in L_j, d. h. $p_j(M)$ ist gleich L_j oder gleich o. Falls $p_{j_0}(M) = L_{j_0}$ ist für ein festes j_0, so enthält M das Element e_{j_0} aus P mit den Komponenten

$$p_{j_0}(e_{j_0}) = \text{Einselement von } L_{j_0} \text{ und } p_j(e_{j_0}) = o \text{ sonst};$$

denn ist $p_{j_0}(x) = p_{j_0}(e_{j_0})$ für $x \in M$, so gehört $e_{j_0} = e_{j_0} x$ zu M. Es ist dann $Pe_{j_0} < M$; d. h. in M liegen alle Elemente y mit Komponenten

$$p_j(y) = \begin{cases} o \text{ für } j \neq j_0 \\ \text{ein beliebiges Element von } L_{j_0} \text{ für } j = j_0. \end{cases}$$

Ist $p_j(M) = L_j$ für alle $j \in J$, so kann ich also zu endlich vielen beliebig vorgegebenen Indizes $j_1, \ldots, j_n$ und Elementen $z^{j_1}, \ldots, z^{j_n}$ aus $L_{j_1}, \ldots, L_{j_n}$ ein Element z in M finden, für welches $p_{j_m}(z) = z^{j_m}$, $m = 1, \ldots, n$ gilt, d. h. M ist dicht in P. Insbesondere gibt es zu jedem abgeschlossenen, maximalen, zweiseitigen Ideal N einen Index $j' \in J$ mit $p_{j'}(N) = o$, d. h. N ist gleich dem maximalen zweiseitigen Ideal aller Elemente x aus P, für welche $p_{j'}(x) = o$ ist. Die lineartopologische Algebra P ist nun als topologisches Produkt vollständiger Algebren vollständig und also ist P die vollständige Hülle von S. Die abgeschlossene Hülle $\overline{U}_i$ von U_i in der vollständigen Hülle $\overline{L}$ von L ist ein abgeschlossenes, zweiseitiges Ideal in $\overline{L}$ (§ 1, (12)). Nach dem Beweis von Satz 2 ist L/U_i isomorph $\overline{L}/\overline{U}_i$, d. h. $\overline{U}_i$ ist ein abgeschlossenes, maximales zweiseitiges Ideal in $\overline{L}$ oder zufolge der Isomorphie zwischen $\overline{L}$ und P auch in P; also gilt $p_j(\overline{U}_i) = o$ für ein $j \in J$. Aus $p_j(U_i) = o$ folgt aber $U_i < V_j$, d. h. $U_i = V_j$. Es gilt demnach:

(20) *Ergibt sich $L_j^2 \neq o$ für alle $j \in J$, so war die im Beweis verwendete Auswahl leer, es kommen unter den Idealen V_j wieder alle U_i vor.*

Aus dem erhaltenen Satz folgern wir:

Satz 5. *Eine halbeinfache, linear kompakte Algebra $L(T)$ ist topologisch isomorph einem topologischen Produkt von vollen Matrizenalgebren endlichen Ranges über Schiefkörpern und besitzt also ein Einselement. Ist L kommutativ, so sind an Stelle der Matrizenalgebren Erweitungskörper von K zu setzen.*

Beweis. Nach (17) ist die Voraussetzung von Satz 4 erfüllt. Hier ist S abgeschlossen, d. h. $S = P$. Für $L_{j'}^2 = o$ wäre das Ideal

$$\left(x \text{ aus } P: \; p_j(x) = \begin{cases} o \text{ für } j \neq j' \\ \text{beliebig in } L_{j'} \text{ für } j = j' \end{cases}\right)$$

ein quasireguläres, rechtes Ideal in P, also können keine Nullalgebren als Faktoren auftreten. Deshalb gilt jetzt auch (20). Wenn L kommutativ ist, sind die Matrizen vom Rang 1.

Korollar 1. *Sei $L(T)$ eine vollständige, halbeinfache, kommutative, lineartopologische Algebra mit einer Nullumgebungssubbasis aus maximalen Idealen; dann ist $L(T)$ topologisch isomorph einem topologischen Produkt aus diskreten Körpern und hat ein Einselement.*

Denn ist U_i ein Element der Nullumgebungssubbasis, so ist L/U_i nach [IV], theorem 22. 10. 1, ein Erweiterungskörper von K oder eine Nullalgebra und also ist die Schlußweise von Satz 4 anwendbar. Wie in Satz 5 folgt, daß Nullalgebren als Faktoren nicht in Frage kommen.

Korollar 2. *Eine kommutative, halbeinfache, linear kompakte Algebra $L(T)$ über algebraisch abgeschlossenem Körper K ist topologisch isomorph einer Algebra ω_Δ.*

In der Darstellung von $L(T)$ als Produkt nach Satz 5 wird dann jeder Faktor gleich K.

Korollar 3. *Das Radikal R einer linear kompakten Algebra ist regulär.*

R ist nämlich abgeschlossen (§ 1, Satz 4) und die halbeinfache, linear kompakte Algebra L/R enthält nach Satz 5 ein Einselement.

Korollar 4. *Das Spektrum eines Elementes einer kommutativen, linear kompakten Algebra $L(T)$ über algebraisch abgeschlossenem Körper K ist nicht leer.*

Beweis. Enthält L ein Einselement e, so hat die Gleichung $-e + x - ex = o$ keine Lösung in L, d. h. $-e$ ist nicht quasiregulär und L ist keine Radikalalgebra. Die halbeinfache Algebra L/R ist wegen Korollar 2 eine Algebra ω_d. Wenn ein Element x aus L ein leeres Spektrum hätte, so auch sein Bild $\hat{x}$ in L/R, weil Quasiregularität bei homomorpher Abbildung erhalten bleibt. Dies widerspricht aber § 1, (24). Existiert kein Einselement, so liegt 0 im Spektrum jedes Elementes.

Wir ziehen einige Folgerungen aus Satz 5.

(21) *Jedes abgeschlossene, zweiseitige Ideal G einer halbeinfachen, linear kompakten Algebra $L(T)$ besitzt ein T-komplementäres Ideal H, d. h. es ist $L(T)$ die topologische direkte Summe aus G und H. Das Ideal G ist regulär und besitzt ein Einselement (ebenso H).*

Beweis. Wir identifizieren $L(T)$ mit der Algebra P aus Satz 5. Wenn $p_{i'}(G) \neq o$, d. h. $= L_{i'}$ ist für die Teilindizesmenge $I' < I$, so ist G nach der Ableitung von (20) dicht in dem zweiseitigen Ideal aller Elemente y aus L mit $p_{i''}(y) = o$ für alle $i'' \in I'' = I - I'$, d. h. G ist gleich diesem Ideal. Topologisch komplementär in L ist hierzu das Ideal H, welches aus allen Elementen z von L mit $p_{i'}(z) = o$ für alle $i' \in I'$ besteht. H ist offenbar abgeschlossen in P, also ist H wie G linear kompakt; nach § 1, (20) sind G und H halbeinfach und sie besitzen Einselemente wegen Satz 5.

(22) *Die lineartopologische Algebra $L(T)$ lasse T_s zu und enthalte zwei algebraisch komplementäre, linear kompakte, zweiseitige Ideale H_1 und H_2. Wenn eine der folgenden Bedingungen erfüllt ist:*

a) *L ist halbeinfach,*

b) *H_1 ist halbeinfach,*

c) *L besitzt ein Einselement e,*

d) *H_1 besitzt ein Einselement e_{H_1},*

so sind H_1 und H_2 auch T-komplementär und $L(T)$ ist also linear kompakt.

Beweis. Es folgt b) aus a) nach § 1, (20); Bedingung b) ergibt d) nach Satz 5. Sei $e = e_1 + e_2$, mit $e_1 \in H_1$ und $e_2 \in H_2$; dann ist e_1 Einselement in H_1, weil $H_1 + H_2 = L$ und $H_1 \cap H_2 = o$ zur Folge hat $H_1 H_2 = o$ (die Menge $H_1 H_2$ liegt in H_1 und H_2); also ergibt c) die Bedingung d). Auf H_1 induzieren nun T und T_s wegen (9) und (7) dieselbe Topologie. Sei U eine beliebige Nullumgebung bezüglich T_s in L, die wir als zweiseitiges Ideal ansetzen können. Bezeichne p die Projektion von L auf H_1; dann ist p stetig, denn wenn x ein beliebiges Element aus U ist, $x = x_1 + x_2$, so enthält U auch das Element $e_{H_1} x = x_1$, d. h. es gilt $p(U) < U \cap H_1$. Der Nachweis vollendet sich mit [VIII], § 4, 7. (6).

(23) *Die kommutative, lineartopologische Algebra $L(T)$ enthalte die algebraisch komplementären Ideale G und H; das Ideal G sei linear kompakt und nicht im Radikal von L enthalten. Dann gibt es eine T-komplementäre Zerlegung $L = G^* + H^*$, wo $G^* < G$ linear kompakt ist; außerdem ist $G/R(G)$ isomorph $G^*/R(G^*)$, wenn $R(G)$ das Radikal von G bedeutet.*

Beweis. $R(G)$ ist nicht gleich G (nach § 1, (20)) und regulär in G. Wir zeigen, daß es ein idempotentes Einselement modulo $R = R(G)$ in G gibt. Sei c_0 ein beliebiges solches Einselement, d. h. $(c_0^2 - c_0) \in R$. Wir übernehmen aus [VI], lemma 12, den Ansatz

$$c_n = 3c_{n-1}^2 - 2c_{n-1}^3, \quad n = 1, 2, \ldots,$$

und die Folgerung

$$c_n^2 - c_n = 4(c_{n-1}^2 - c_{n-1})^3 - 3(c_{n-1}^2 - c_{n-1})^2,$$

welche $(c_n^2 - c_n) \in (R^{2^n})$ ergibt. Nach (19) gibt es zu jeder Nullumgebung U von G eine ganze Zahl k mit $R^k < U$. Hiermit zeigt sich, daß die Folge c_n eine Cauchyfolge in G ist: Schreiben wir R_n für das allgemeine Element aus dem Ideal (R^{2^n}) in G. Dann ist

$$\begin{aligned} c_n &= c_{n-1}^2 - 2c_{n-1}(c_{n-1}^2 - c_{n-1}) = c_{n-1}^2 + R_{n-1} \\ &= (c_{n-2}^2 + R_{n-2})^2 + R_{n-1} = c_{n-2}^{2^2} + R_{n-2} \\ &= \cdots \\ &= c_{n-l}^{2^l} + R_{n-l}. \end{aligned}$$

Für $m < n$ ist also $c_n - c_m = c_m^{2^{n-m}} + R_m - c_m$. Nun gilt

$$c_m^h - c_m = c_m^{h-2}(c_m^2 - c_m) + c_m^{h-3}(c_m^2 - c_m) + \cdots + (c_m^2 - c_m) = R_m,$$

d. h. $c_n - c_m = R_m$. Für alle $n, m > k$ gilt demnach $(c_n - c_m) \in U$, und c_n ist eine Cauchyfolge in G. Wenn sie gegen das Element c von G konvergiert, so konvergiert $c_n^2 - c_n$ gegen o und gegen $c^2 - c$, d. h. c ist idempotent. Nach der Konstruktion von c_n liegt dieses Element stets in der Restklasse $c_0 + R$, also gehört auch c zu der mit R abgeschlossenen Menge $c_0 + R$, d. h. c ist ein Einselement modulo R. — Mit Hilfe von c zerlegen wir G in $G = cG + (G - cG)$, wo $(G - cG)$ alle Elemente $x - cx$ mit $x \in G$ bedeutet; cG ist nach (2) linear kompakt und hat das Einselement c. Die Algebra L zerfällt,

$$\begin{aligned} L &= \underbrace{cG} + \underbrace{(G - cG) + H} \\ &= G^* + \quad H^* \quad . \end{aligned}$$

Das Ideal G^* von G ist auch ein Ideal in L, weil $c \in G^*$ idempotent ist und xc in G, d. h. $xcc = xc$ in G^* liegt für $x \in L$. Die Menge H^* ist ein Ideal in L, da G und H Ideale sind. Sei nun p die Projektion von L auf G^*; wegen $p(x) = cx$ für alle $x \in L$ ist p stetig und daher die Zerlegung T-komplementär ([VIII], § 4, 7. (6)). Schließlich ist $(G - cG) < R(G)$ und deshalb $G/R(G)$ isomorph $G^*/R(G) \cap G^* = G^*/R(G^*)$ (mit § 1, (20)).

Ein lineartopologischer Raum heißt *lokal linear kompakt*, wenn er eine linear kompakte Nullumgebung U besitzt. Ist eine lineartopologische Algebra als Raum lokal linear kompakt, so heiße sie eine lokal linear kompakte Algebra; hier gibt es eine offene, linear kompakte Subalgebra U.

Satz 6. *Eine halbeinfache, lokal linear kompakte Algebra $L(T)$ ist genau dann idealtopologisch, wenn es in $L(T)$ ein linear kompaktes, zweiseitiges, offenes Ideal G gibt. Dann ist L die topologische direkte Summe aus G und einem diskreten, halbeinfachen, zweiseitigen Ideal H, also $L = G + H$.*

Beweis. Sei ein solches Ideal G vorhanden. Nach § 1, (20) ist G halbeinfach und hat wegen Satz 5 ein Einselement e, d. h. es gilt (12). Setzen wir umgekehrt eine Nullumgebungsbasis aus zweiseitigen Idealen voraus, so gibt es in L ein offenes, zweiseitiges Ideal G, welches in U enthalten ist. G ist abgeschlossen in U, also linear kompakt. — Ferner ist L die direkte Summe von $eL = G$ und $H = (L - eL)$; da $ex = exe = xe$ gilt für jedes $x \in L$, ist H ebenfalls ein zweiseitiges Ideal und die direkte Summe gilt auch im Sinn des Ringproduktes. Sie ist T-topologisch, weil der Summand G offen ist. H ist isomorph L/G, also ist H diskret.

Mit Satz 5 erhalten wir:

Satz 7. *Sei $L(T)$ eine idealtopologische, halbeinfache, lokal linear kompakte Algebra, und jedes Element x aus L sei in einem linear kompakten, zweiseitigen Ideal G_x enthalten. Dann ist L die topologische direkte Summe der Ideale G und H aus Satz 6 und G ist topo-*

logisch isomorph einem topologischen Produkt von vollen Matrizenalgebren endlichen Ranges über Schiefkörpern, während H topologisch isomorph ist einer topologischen direkten Summe aus ebensolchen Matrizenalgebren.

Beweis. Für ein Element x aus H ist $H_x = G_x \cap H$ ein linear kompaktes, halbeinfaches, zweiseitiges Ideal in H, d. h. H_x ist endlichdimensional (vgl. (3)) und besitzt ein Einselement. Jedes Element x aus H ist also in einem endlichdimensionalen, zweiseitigen Ideal mit Einselement von H enthalten. M bedeute eine Menge von endlichdimensionalen, zweiseitigen Idealen mit Einselement aus H, von denen je zwei den Durchschnitt o haben und A sei die Gesamtheit solcher Mengen M aus H. In A führen wir eine Halbordnung bezüglich $<$ ein; dann ist die Vereinigungsmenge einer geordneten Teilmenge aus A in A enthalten. Nach Zorn gibt es in A ein maximales Element M. Die lineare Hülle (M) ist ein zweiseitiges Ideal in H, von dem wir $(\mathsf{M}) = H$ behaupten. Für x aus dem Komplement von (M) in H ist $H_x \cap (\mathsf{M})$ ein halbeinfaches, endlichdimensionales, zweiseitiges Ideal in H_x, also gibt es wegen (21) ein komplementäres Ideal N dazu in H_x, und N ist auch ein endlichdimensionales, zweiseitiges Ideal in H, weil N ein Einselement enthält. Wegen $N \cap (\mathsf{M}) = N \cap H_x \cap (\mathsf{M}) = o$ gehört $N \cup \mathsf{M}$ zu A, so daß für $x \neq o$ (und damit $N \neq o$) die Menge M nicht maximal wäre. — Jedes der endlichdimensionalen, zweiseitigen Ideale mit Einselement aus M zerfällt (da es wegen § 1, (20) halbeinfach ist) nach Satz 5 in eine Summe von endlich vielen vollen Matrizenalgebren endlichen Ranges über Schiefkörpern; dies beweist die über Satz 6 hinausgehende Behauptung unseres Satzes.

Ein lokal linear kompakter Raum $L(T)$ läßt sich stets auffassen als topologische direkte Summe aus einem linear kompakten und einem diskreten linearen Raum, $L = U + V$, wo V ein algebraischer Komplementärraum von U ist; deshalb ist dieser Raum vollständig. Nach § 1, Satz 4, ist also das Radikal einer lokal linear kompakten Algebra $L(T)$ abgeschlossen, wenn $L(T)$ idealtopologisch ist. Es gilt aber sogar:

Satz 8. *Das Radikal einer lokal linear kompakten Algebra $L(T)$ ist stets abgeschlossen.*

Beweis. Die abgeschlossene Hülle $\bar{R}$ des Radikals R von L ist ein abgeschlossenes, zweiseitiges Ideal in L. Darum ist $\bar{R}$ eine lokal linear kompakte Algebra und enthält also eine (in $\bar{R}$) offene, linear kompakte Subalgebra H mit Radikal S.

Ist $R \neq \bar{R}$, d. h. $\bar{R}$ keine Radikalalgebra, so wollen wir zunächst nachweisen, daß es in $\bar{R}$ ein abgeschlossenes, reguläres, maximales einseitiges Ideal M gibt. Im Fall $H = S$ läßt sich dies fast wörtlich wie in [IV] auch bei unserer Definition von „quasiregulär" schließen: Wegen theorem 22. 14. 2 gibt es in $\bar{R}$ ein einseitiges, reguläres, maximales Ideal M, das nach theorem 22. 10. 4 abgeschlossen ist. — Sei nun $H \neq S$. Zunächst ist S abgeschlossen in H, sowie H/S halbeinfach und linear kompakt, also ist H/S ein topologisches Produkt von vollen Matrizenalgebren endlichen Ranges über Schiefkörpern. Das Element $\hat{u}$ aus H/S habe alle Komponenten o außer etwa der k-ten, welche gleich dem Einselement 1 der entsprechenden Matrizenalgebra sei. Dann führt die Linksmultiplikation mit $\hat{u}$ in H/S das offene, zweiseitige Ideal V aller Elemente aus H/S, deren k-te Komponente o ist, in o über. Wie im Beweis von (23) gibt es ein idempotentes Urbild u von $\hat{u}$ in H und es ist $up^{(-1)}(V)\, u = uWu < S$, wo p den Homomorphismus von H auf H/S kennzeichnet; W ist eine Nullumgebung in H, d. h. in $\bar{R}$. Das Element $-u$ ist nicht rechts quasiregulär in $\bar{R}$; denn multipliziert man $-u + y - uy = o$ mit u von links her, so erhält man den Widerspruch $-u = o$. Deshalb enthält das reguläre, rechte Ideal $(x - ux)$, wo x über $\bar{R}$ läuft, u nicht; d. h. es ist eigentlich in $\bar{R}$ und kann wie in [IV], theorem 22. 14. 3, eingebettet werden in ein reguläres, maximales rechtes Ideal M mit linker Einheit u modulo M.

Ist M dicht in $\bar{R}$, so enthält die Umgebung $u + W$ von u ein Element aus M, also gibt es in M ein Element $u + x$ mit $x \in W$. Zu uxu gibt es nach Definition von W eine rechte Quasiinverse y in $\bar{R}$ (mit $y \in S$). Für $z = (u + x)(u + uy)$ gilt dann

$$uz = u(u + uy + xu + xuy) = u + u(y + uxu + uxuy) = u$$

und z liegt (mit $u + x$) ebenso wie $z - uz$ in M; daraus folgt $uz = u \in M$ und $M = \bar{R}$ (als Vorlage für diese Schlußweise diente mir der Beweis von [VII], theorem 11). Der erhaltene Widerspruch zeigt, daß M abgeschlossen ist in $\bar{R}$. Das Radikal R von $\bar{R}$ (vgl. § 1, (20)) ist enthalten in M, denn sonst umfaßt das rechte Ideal $M + R$ das maximale rechte Ideal M, d. h. $M + R$ ist gleich $\bar{R}$ und es gibt also in R ein zu u modulo M kongruentes Element a; das Element a ist dann ebenfalls ein linkes Einselement modulo M in $\bar{R}$. Ist b die Quasiinverse von $(-a) \in R$, so gilt $b - ab = a$, woraus $a \in M$ und $M = \bar{R}$ folgt.

Es hat sich also ergeben, daß die in $\bar{R}$ dichte Menge R zugleich in dem in $\bar{R}$ abgeschlossenen, eigentlichen Ideal M enthalten ist; der Widerspruch erweist die Unrichtigkeit unserer Annahme $R \neq \bar{R}$.

§ 3. Homomorphe Abbildungen auf den Grundkörper K.

Die Gesamtheit der T-stetigen (algebraisch) homomorphen Abbildungen einer lineartopologischen Algebra $L(T)$ in K wollen wir mit $M(L)$ bezeichnen; $M(L)$ ist also ein Teilraum von L', dem zu L dualen Raum. $M^-(L)$ sei $M(L)$ ohne die Nullabbildung Θ. Natürlich kann man nur in speziellen lineartopologischen Algebren ein nicht leeres $M^-(L)$ erwarten. Die Existenz einer nichttrivialen, homomorphen Abbildung einer lineartopologischen Algebra $L(T)$ in den Grundkörper K ist gleichbedeutend mit dem Vorhandensein eines abgeschlossenen, zweiseitigen Ideals H, dessen Restklassenalgebra isomorph K ist. Wir wollen die Struktur der hier zu betrachtenden lineartopologischen Algebren $L(T)$ gleich noch etwas mehr einengen und fordern, daß es zu zwei verschiedenen Elementen x und y aus L ein solches Ideal H mit $L/H \cong K$ gibt, daß x und y verschiedenen Restklassen modulo H angehören. Auf $M(L)$ übertragen bedeutet dies: Es gibt ein $f \in M(L)$ mit $f(x) \neq f(y)$ (es ist $H = f^{(-1)}(0)$), oder $M(L)$ *trennt*. Als Beispiele lineartopologischer Algebren mit trennendem $M(L)$ nennen wir φ_d, ω_d und die Algebren abzählbarer Stufe. Hier sind die Projektionen p_i Elemente von $M(L)$; für φ_d und ω_d auch nur diese:

(1) *Die einzigen homomorphen Abbildungen von φ_d auf K sind die Projektionen p_i.*

Beweis. Ist f eine homomorphe Abbildung von φ_d auf K, so ist $f^{(-1)}(0)$ ein maximales Ideal H in φ_d und also nach § 2, (15) gegeben durch eine Bedingung $x_j = 0$. Dann ist $f = p_j$.

(2) *In ω_d sind die abgeschlossenen, maximalen Ideale gekennzeichnet durch eine Bedingung $x_i = 0$; also gibt es auch von ω_d außer den Projektionen p_i keine stetigen, homomorphen Abbildungen auf K.*

Der Beweis verläuft wörtlich wie die erste Hälfte des Beweises von § 2, (20); die dort L_j genannten Algebren sind hier alle gleich K und statt P ist ω_d zu setzen.

Aus dem Beweis folgt, daß ein Ideal H aus ω_d dicht ist in ω_d, wenn $p_i(H) \neq 0$ ist für alle i aus der Komponentenindizesmenge I. Wie es schon im Beweis von § 2, (21) geschehen ist, können wir uns auf eine Teilindizesmenge I' von I beschränken: Sei G ein beliebiges Ideal aus ω_d und genau für die Indizes $i' \in I'$ gebe es ein Element x in G mit nichtverschwindender i'-ter Komponente. Dann enthält G die „Einheitsvektoren" $e_{i'}$ (vgl. Beweis von § 2, (20)) und ist deshalb dicht in dem Ideal $\tilde{G}$ aller Elemente von ω_d, deren Komponenten 0 sind für die Indizes aus $I - I'$. Das Ideal $\tilde{G}$ ist offenbar abgeschlos-

sen in ω_d. Also gilt: Genau die Ideale aus ω_d sind abgeschlossen, welche durch Bedingungen $x_{i''} = 0$ für alle i'' aus I'' gekennzeichnet werden können. Da ein endlichdimensionales Ideal einer lineartopologischen Algebra abgeschlossen ist (§ 1, (5)), sind in φ_d und ω_d die endlichdimensionalen Ideale so gekennzeichnet: Es gibt Indizes $i_1, \ldots, i_n$, so daß das Ideal gerade aus allen Elementen x von L mit Komponenten

$$x_i = \begin{cases} 0 \text{ für } i \neq i_k,\ k = 1, \ldots, n \\ \text{beliebig sonst} \end{cases}$$

besteht. Durch zusätzliche Voraussetzungen kann man erreichen, daß (2) für alle homomorphen Abbildungen von ω_d auf K gilt:

(3) *Hat K wenigstens die Mächtigkeit d, so gibt es außer den Projektionen p_i keine homomorphen Abbildungen von ω_d auf K.*

Zum Beweis benötigen wir folgende Aussage:

(4) *Das Bild eines Elementes x aus der Algebra L bei einer nichttrivialen, homomorphen Abbildung f auf K gehört stets zum Spektrum von x.*

Beweis. Wenn $f(x) = 0$ ist, kann x nicht regulär sein; denn aus $xx^{-1} = e$ folgt $f(e) = 1 = f(x)\,f(x^{-1})$, weil jede homomorphe Abbildung das Einselement e in 1 überführt. Ist $f(x) = r \neq 0$, so ist $-\frac{1}{r}x$ nicht rechts quasiregulär, wie man durch Anwendung von f auf die Gleichung $y - \frac{1}{r}x - \frac{1}{r}xy = 0$ sieht.

Nun zum Beweis von (3): Sei f eine beliebige homomorphe Abbildung von ω_d auf K. Dann gehört $f(x)$ für jedes feste Element x zum Spektrum von x, d. h. wegen § 1, (24) ist $f(x) = p_i(x)$ für einen passenden Index $i \in I$. Da e_i idempotent ist, haben wir $f(e_i) = 1$ oder $f(e_i) = 0$. Im ersten Fall folgt

$$f(x) = f(xe_i) = f(p_i(x)\,e_i) = p_i(x)$$

für alle $x \in \omega_d$. Wenn jedoch f für alle e_i verschwindet und y ein Element aus ω_d ist mit paarweise verschiedenen Komponenten, und es ist $f(y) = y_j$, so gilt

$$f(y + e_j) = f(y) + f(e_j) = y_j.$$

y_j kommt aber unter den Komponenten von $y + e_j$ nicht mehr vor; dies ist nach dem oben Gesagten unmöglich.

Untersuchen wir nun lineartopologische Algebren $L(T)$ mit trennendem $M(L)$! Wenn wir dabei auf $M(L)$ eine Topologie verwenden, so handelt es sich stets um die durch die schwache Topologie $T_s(L)$ von L' in $M(L)$ induzierte Topologie.

Satz 1. *Hat die lineartopologische Algebra $L(T)$ ein trennendes $M(L)$, so ist L algebraisch isomorph einer Subalgebra L^* von ω_d, wo d die Mächtigkeit von $M^-(L)$ bedeutet; die Algebra L ist also kommutativ und sie ist halbeinfach. $M(L)$ ist abgeschlossen in $L'(T_s(L))$ und die abgeschlossene, lineare Hülle von $M(L)$ in L' ist gleich L'. Besitzt L ein Einselement, so ist die Nullabbildung in $M(L)$ isoliert.*

Beweis. Wenn f_i, mit $i \in I$, die Menge $M^-(L)$ durchläuft, so bildet die Zuordnung $x \to (f_i(x))$ die Algebra L isomorph ab auf die Subalgebra L^* von ω_d; die Elemente f_i aus $M^-(L)$ sind dabei die Projektionen p_i von L^*. Die Algebra L^* ist halbeinfach, weil es zu jedem Element $y \neq o$ aus L^* nach Voraussetzung eine Projektion p_i mit $p_i(y) = r \neq 0$ gibt; r liegt dann im Spektrum von y und es ist also $-\frac{1}{r}y$ nicht quasiregulär. — Für feste Elemente x und y aus L ist die Abbildung

$$f \to f(xy) - f(x)\,f(y), \quad \text{für } f \in L',$$

nach Definition der schwachen Topologie eine stetige Abbildung von $L'(T_s)$ in K. Deshalb ist

$$M(L) = \bigcap_{x,\,y \text{ aus } L} (f \text{ aus } L' : \; f(xy) - f(x)\,f(y) = 0)$$

als Durchschnitt von abgeschlossenen Mengen, nämlich der Nullräume stetiger Abbildungen, ebenfalls abgeschlossen. — Nun wollen wir zeigen, daß die abgeschlossene lineare Hülle von $M(L)$ gleich L' ist; sie ist gleich der abgeschlossenen Hülle $\overline{(M(L))}$ der linearen Hülle $(M(L))$ von $M(L)$ in L', weil $\overline{(M(L))}$ nach § 1, (8) linear ist. Wir müssen also in jeder Umgebung U eines Elementes u von $L'(T_s(L))$ eine Linearkombination von Elementen aus $M(L)$ angeben. Wir können uns U durch n linear unabhängige Elemente $x^1, \ldots, x^n$ aus L als Gesamtheit der Elemente f aus L' erklärt denken, für welche $f(x^\nu) = u(x^\nu)$ ist, $\nu = 1, \ldots, n$. Man überlegt sich leicht, daß es zu n linear unabhängigen Elementen $x^1, \ldots, x^n$ aus L^* stets Projektionen p_{i_ν}, $\nu = 1, \ldots, n$ in L^* gibt, so daß die Vektoren

$$\begin{pmatrix} p_{i_1}(x^1) \\ \cdot \\ \cdot \\ \cdot \\ p_{i_1}(x^n) \end{pmatrix}, \ldots, \begin{pmatrix} p_{i_n}(x^1) \\ \cdot \\ \cdot \\ \cdot \\ p_{i_n}(x^n) \end{pmatrix}$$

linear unabhängig sind. Den Vektor

$$\begin{pmatrix} u(x^1) \\ \cdot \\ \cdot \\ \cdot \\ u(x^n) \end{pmatrix}$$

können wir somit als Linearkombination mit Koeffizienten $r_1, \ldots, r_n$ aus den angegebenen Vektoren darstellen; d. h. das Element $\sum_{\nu=1}^{n} r_\nu p_{i_\nu}$ liegt in U. — Schließlich ist die Nullabbildung Θ das einzige Element von $M(L)$, das in der in $L'(T_s(L))$ offenen Menge $e^\perp$ liegt.

Die Elemente x aus L sind stetige Abbildungen von $M(L)$ in K und diese verschwinden natürlich für die Nullabbildung Θ. Es liegt nahe, die Algebra $C_0(M(L))$ der für Θ verschwindenden stetigen Abbildungen von $M(L)$ in K zu betrachten (Summe und Produkt seien in C_0 punktweise erklärt).

Satz 2. *Jede lineartopologische Algebra mit trennendem $M(L)$ läßt sich isomorph abbilden auf eine trennende Subalgebra C_L von $C_0(M(L))$. Die Isomorphie wird stetig, wenn man in C_0 die Topologie der einfachen Konvergenz (dann genügt $T_s(L')$ auf L) oder die der uniformen Konvergenz in den äquistetigen Teilmengen* (vgl. [II], § 3, définition 1) *von $M(L)$ wählt. Die Isomorphie ist topologisch für die diskrete Topologie in L und die Topologie der uniformen Konvergenz auf $M(L)$ in $C_0(M(L))$.*

Nach § 1, Satz 7, Korollar, ist $C_0(M(L))$ bezüglich der angegebenen Topologien jeweils ein lineartopologischer Raum.

Beweis. Die Zuordnung $h: x \to h_x$, wo $h_x(f) = f(x)$ ist für alle $f \in M(L)$, gibt uns eine homomorphe Abbildung von L auf C_L, und C_L trennt. Weil $M(L)$ trennt, folgt aus $h_x = o$, d. h. $f(x) = 0$ für alle $f \in M(L)$, daß x das Nullelement von L ist; d. h. diese Zuordnung ist eine Isomorphie. Eine Nullumgebung U einer Nullumgebungsbasis bezüglich der Topologie der einfachen Konvergenz besteht aus allen Elementen g von C_0,

welche endlich viele Elemente $f_1, \ldots, f_n$ aus $M(L)$ in 0 abbilden. Die schwache Nullumgebung $(f_1, \ldots, f_n)^\perp$ in L wird von h in einen Teil von U übergeführt. Äquistetig in o sind in L' gerade die Orthogonalräume $V^\perp$ von Nullumgebungen V aus L und die Teilmengen solcher Mengen $V^\perp$; in $M(L)$ sind also die Mengen $V^\perp \cap M(L)$ äquistetig, und eine Nullumgebungsbasis von C_L bezüglich der Topologie der uniformen Konvergenz in diesen Durchschnitten ist gegeben in den Mengen

$$W_{V^\perp} = \big(y \text{ in } C_L\colon\ y(f) = 0 \text{ für alle } f \text{ aus } V^\perp \cap M(L)\big).$$

Es liegt $h(V)$ in $W_{V^\perp}$, d. h. h ist stetig. Endlich ist die Topologie der uniformen Konvergenz auf $M(L)$ in $C_0(M(L))$ offenbar die diskrete Topologie.

Eine lineartopologische Algebra $L(T)$ heißt *voll*, wenn $C_L = C_0(M(L))$ ist.

(5) *Die Algebren φ_d und ω_d sind voll.*

Denn wenn g ein Element aus $C_0(M(\varphi_d))$ ist, so gibt es eine Umgebung U von Θ in $M(\varphi_d)$, welche durch g in 0 abgebildet wird. Jede Nullumgebung in $M(\varphi_d)$ enthält nun nach Konstruktion der schwachen Topologie und wegen (1) alle Elemente von $M(\varphi_d)$ bis auf endlich viele; etwa die Projektionen $p_{i_1}, \ldots, p_{i_n}$ seien nicht in U gelegen. Dann leistet das Element x aus φ_d mit den Komponenten $x_{i_k} = g(p_{i_k})$ für $k = 1, \ldots, n$, und $x_i = 0$ sonst, dieselbe Abbildung wie g. — Im Fall von ω_d induziert $T_s(L)$ in $M(\omega_d)$ die diskrete Topologie; denn $p_i \neq \Theta$ ist isoliert, da das Element e_i in ω_d liegt und die Umgebung

$$U(p_i) = \big(f \text{ aus } M(\omega_d)\colon\ f(e_i) = p_i(e_i) = 1\big)$$

von p_i in $M(\omega_d)$ wegen (2) nur p_i selbst enthält; und Θ ist nach Satz 1 ein isoliertes Element, weil ω_d ein Einselement besitzt.

Allgemeiner gilt:

(6) *Die lineartopologische Algebra $L(T)$ sei vollständig und habe eine Nullumgebungsbasis (U_i), mit $i \in I$, aus zweiseitigen Idealen; wenn jede Algebra $L_i = L/U_i$ voll ist, so ist auch L voll* (L ist dann kommutativ).

Beweis. Sei $z \in C_0(M(L))$ und $z(i)$ bedeute die Restriktion von z auf $M(L) \cap U_i^\perp$. Man kann $M(L) \cap U_i^\perp$ und $M(L_i)$ topologisch isomorph aufeinander abbilden: Wenn f in $M(L) \cap U_i^\perp$ liegt, so ist f eine homomorphe Abbildung f_i der diskreten Algebra L_i auf K mit $f_i(p_i(x)) = f_i(x_i) = f(x)$, wo p_i die Abbildung von L auf L_i ist; und die Zuordnung $f_i \longleftrightarrow f$ ist eine eineindeutige, bezüglich $T_s(L_i)$ und $T_s(L)$ topologisch isomorphe Abbildung von $M(L) \cap U_i^\perp$ auf $M(L_i)$, da für $g \in M(L_i)$ die Abbildung gp_i zu $M(L) \cap U_i^\perp$ gehört. Bei dieser Isomorphie sei $z(i)$ das Element $x(i)$ zugeordnet; $x(i)$ liegt nach Voraussetzung in L_i. Für $U_j < U_i$ ist $U_i^\perp \cap M(L) < U_j^\perp \cap M(L)$ und es ist $x(i) = x(j)\,(i)$; verwenden wir die Bezeichnungsweise aus § 1, Satz 3, so ist also $x(i) = f_{ij}(x(j))$ für $i \leqq j$, denn ein Element aus einem L_i ist bestimmt durch die Abbildung, die es auf $M(L_i)$ erzeugt. Nach jenem Satz gibt es in L ein Element x mit $x_i = x(i)$ für alle $i \in I$, d. h. es ist $f(x) = f_i(x_i) = x(i)\,(f_i) = z(f)$ für $f \in U_i^\perp \cap M(L)$. Jedes Element f von $M(L)$ liegt in einer Menge $U_i^\perp \cap M(L)$, so daß x und z in f übereinstimmen, d. h. z liegt in C_L.

(7) *Sei $L(T)$ das topologische Produkt von lineartopologischen Algebren L_i; dann ist $M(L)$ die Vereinigung der Mengen G_i, wo G_i aus allen Homomorphismen der Gestalt $f_{ij}p_i$, $(f_{ij}p_i(x) = f_{ij}(p_i(x)))$, mit $f_{ij} \in M(L_i)$ besteht.*

Beweis. Topologisch isomorph zu L_i ist in L die Subalgebra L^i aller Elemente x^i, deren Komponenten $p_j(x^i) = x_j^i$ Null sind für $j \neq i$. Wenn g ein Element von $M(L)$ ist, so kann g nicht alle Algebren L^i in 0 überführen, denn die direkte Summe der L^i ist

dicht und $g^{(-1)}(0)$ ist abgeschlossen in $L(T)$. Ist $g(L^i) \neq 0$ für ein bestimmtes i, so gibt es ein Element x^i in L^i, so daß $g(x^i) = 1$ ist. Es folgt für jedes $x \in L$

$$g(x) = g(xx^i) = g(p_i(x)\, x^i);$$

g hat also für zwei Elemente aus L mit gleicher i-ter Komponente denselben Wert. $p_i(x)$ läuft über L_i, wenn x in L variiert; d. h. durch

$$f_{ij}(p_i(x)) = g(x), \text{ also } f_{ij}p_i = g$$

ist eine homomorphe Abbildung f_{ij} von L_i in K erklärt; sie ist stetig in L_i, weil p_i offen ist. — Andererseits gehört auch jeder Homomorphismus $f_{ij}p_i$ zu $M(L)$.

Ganz analog beweist sich (7) für die topologische direkte Summe an Stelle des topologischen Produktes.

Hieraus folgt:

Satz 3. *Ein topologisches Produkt voller Algebren ist voll; dasselbe gilt für die topologische direkte Summe voller Algebren.*

Denn wegen $f_{ij}p_i(x) = f_{ij}(x_i)$ für alle x aus dem topologischen Produkt L sind G_i und $M(L_i)$ in der Zuordnung $f_{ij}p_i \leftrightarrow f_{ij}$ homöomorph bezüglich T_s. Liege nun z in $C_0(M(L))$, und $z(i)$ sei die Restriktion von z bezüglich G_i. Dann existiert nach Voraussetzung für jeden Index i ein Element x_i aus L_i mit $x_i(f_{ij}) = z(i)\,(f_{ij}p_i)$; das Element x in L mit den Komponenten x_i stimmt also auf ganz $M(L)$ mit z überein. — Bedeutet L die topologische direkte Summe der Algebren L_i, so enthält jede Nullumgebung in $M(L)$ alle Mengen G_i mit Ausnahme endlich vieler. Für ein Element z aus $C_0(M(L))$ kann man deshalb (wie in (5)) stets ein Element x in L finden, welches auf ganz $M(L)$ dieselbe Abbildung hervorruft wie z.

$M^-(K)$ besteht nur aus der identischen Abbildung von K auf sich: Liegt f in $M^-(K)$, so ist $f(1) = 1$, also $f(r) = r$ für alle Elemente r aus K. Auch ist K offenbar voll. Die Aussagen von (7) und von Satz 3 sind also Verallgemeinerungen von (2) (bzw. auch (1)) und (5).

Wir vermerken, daß eine volle lineartopologische Algebra nicht notwendig vollständig ist. Denn φ ist ersichtlich auch voll bezüglich der durch ω induzierten Topologie T_i, da $M(L)$ beim Übergang von φ zu $\varphi(T_i)$ erhalten bleibt und dann die schwache Topologie auf $M(L)$ in beiden Fällen dieselbe ist; $\varphi(T_i)$ ist dicht in ω, also nicht vollständig.

Bei vollen lineartopologischen Algebren läßt sich die Aussage (4) verschärfen. Zunächst gilt:

(8) *In einer vollen lineartopologischen Algebra $L(T)$ ist ein Element x genau dann quasiregulär, wenn $f(x) \neq -1$ ist für alle $f \in M(L)$.*

Beweis. Die Notwendigkeit gilt, weil Quasiregularität bei homomorpher Abbildung erhalten bleibt und -1 nicht quasiregulär ist in K. Ist umgekehrt $f(x) \neq -1$ für alle Elemente f von $M(L)$, so hat x als Element von L^* eine Quasiinverse x' in ω_d (vgl. § 1, (24)). Sei $g \in M(L)$ und $x(g) = r$; dann gibt es eine ganze Umgebung U von g in $M(L)$ mit $x(U) = r$. Das Element x' von ω_d kann als Abbildung von $M(L)$ in K aufgefaßt werden, indem man $x'(f)$ für $f \in M^-(L)$ gleich dem Wert der Komponente von x' setzt, die f in der Zuordnung $L \leftrightarrow L^*$ (vgl. Satz 1) entspricht, und $x'(\Theta) = 0$ setzt. Nach Konstruktion von x' (vgl. § 1, (24)) nimmt x' dann auf ganz U denselben Wert an $\left(\text{nämlich } -\dfrac{r}{1+r}\right)$, d. h. x' ist stetig und gehört zu $C_0(M(L))$.

Nun erhalten wir:

Satz 4. *Wenn $L(T)$ eine volle lineartopologische Algebra ist, dann besteht das Spektrum eines Elementes x von L gerade aus allen Skalaren $f(x)$, wo f über $M^-(L)$ läuft.*

Beweis. Im Anschluß an (4) ist noch nachzuweisen, daß nur die Skalare $f(x)$ im Spektrum des Elementes x liegen. Ist $r \neq 0$ ein von allen $f(x)$ verschiedener Skalar, so ist $f\left(-\frac{1}{r}x\right) \neq -1$ für alle $f \in M(L)$, d. h. $-\frac{1}{r}x$ ist nach (8) quasiregulär; also gehört r nicht zum Spektrum von x. Wenn $f(x) \neq 0$ ist für alle $f \in M^-(L)$, so gibt es in ω_d ein Inverses x^{-1} des Elementes x von L^*; man schließt wie eben in (8), daß x^{-1} ein Element der vollen Algebra $L(T)$ ist: Wenn $x(U) = s(\neq 0)$ ist für eine Umgebung U eines beliebigen Elementes g aus $M^-(L)$, so hat x^{-1} auf ganz U den Wert $\frac{1}{s}$, deshalb ist x^{-1} stetig in g. Andererseits gehört nur Θ selbst zur in $M(L)$ offenen Menge $x^{(-1)}(0)$; dieses Element ist demnach isoliert in $M(L)$ und somit x^{-1} auch stetig in Θ erklärbar durch $x^{-1}(\Theta) = 0$. Das Element x ist in diesem Fall also regulär in L und das Spektrum von x enthält 0 nicht. — Die letzte Schlußweise zeigt auch: Besitzt eine volle Algebra $L(T)$ kein Einselement, so gibt es zu jedem Element y aus L eine Abbildung $f \in M^-(L)$, so daß $f(y) = 0$ ist.

Spezielle volle lineartopologische Algebren lassen sich durch die topologischen Eigenschaften von $M(L)$ algebraisch charakterisieren:

(9) *Seien $L_1(T_1)$ und $L_2(T_2)$ zwei volle lineartopologische Algebren, und jede homomorphe Abbildung von L auf K sei stetig. $M(L_1)$ und $M(L_2)$ sind dann und nur dann homöomorph, wenn $C_0(M(L_1))$ und $C_0(M(L_2))$ als Algebren über K isomorph sind.*

Beweis. Die eine Hälfte unserer Aussage ist offensichtlich und wurde bereits verwendet. Wir beweisen noch, daß sie hinreicht. Nach Voraussetzung besteht eine eineindeutige Zuordnung zwischen den Elementen von M und den maximalen Idealen von C_0 mit zu K isomorpher Restklassenalgebra. Sind also $C_0^1 = C_0(M(L_1))$ und $C_0^2 = C_0(M(L_2))$ isomorph, $C_0^2 = h(C_0^1)$, so sind dadurch $M(L_1)$ und $M(L_2)$ eineindeutig aufeinander bezogen, $g = h(f)$, mit $f \in M(L_1)$ und $g \in M(L_2)$, wenn $h(f^\perp) = g^\perp$ ist. Da $C_0^1/f^\perp$ und $C_0^2/g^\perp$ beide isomorph K sind, und K nur die Identität als Automorphismus hat, nehmen f und g auf bei h sich entsprechenden Elementen gleiche Werte an,

$$f(x) = g(h(x)) \text{ für } x \in C_0^1.$$

Diese Gleichung zeigt, daß h ein topologischer Isomorphismus bezüglich T_s ist*).

Die zusätzliche Bedingung von (9) ist von selbst erfüllt im kompakten Fall:

(10) *Wenn die lineartopologische Algebra $L(T)$ voll und $M(L)$ kompakt ist, so ist jedes maximale Ideal H in L von der Form $f(x) = 0$, wo f ein Element aus $M(L)$ ist. Jede homomorphe Abbildung von L auf K ist also stetig.*

Beweis. Nehmen wir an, H enthalte zu jedem Element f ein Element x mit $f(x) \neq 0$. Wenn y ein beliebiges Element von L ist, so gibt es eine offene und abgeschlossene Nullumgebung U in $M(L)$, welche durch y in 0 übergeführt wird. Das Komplement V von U in $M(L)$ ist kompakt, und die Restriktionen der Elemente aus L bezüglich V bilden eine Algebra $\tilde{L}$ stetiger Abbildungen von V in K. Wenn wir nachweisen können, daß das Bild $\tilde{H}$ von H bei der Zuordnung von L auf $\tilde{L}$ die Abbildung $\tilde{u}$ identisch 1 von V in K enthält, also $\tilde{H} = \tilde{L}$ ist, so sind wir fertig; denn ist dann u ein Urbild von $\tilde{u}$ in H, so liegt $yu = y$ in H und es ist $H = L$. Zu einem Element f_1 aus V gibt es nun nach unserer Annahme ein $\tilde{x}_1 \in \tilde{H}$ und eine in V liegende offene und abgeschlossene Umgebung U_{f_1}, so daß $\tilde{x}_1(U_{f_1}) \neq 0$ ist. Die Abbildung $\tilde{y}_1$, welche gleich $\tilde{x}_1^{-1}$ ist in U_{f_1} und gleich 0 im Kom-

*) *Zusatz bei der Korrekur.* (9) bleibt richtig, wenn man C_0^1 und C_0^2 nur als ringisomorph voraussetzt. K hat dann nicht nur die Identität als Automorphismus; die angegebene Gleichung ist durch $f(x) = g(y)$ zu ersetzen, wo y ein passend gewähltes Element von C_0^2 ist.

plement V_{f_1} von U_{f_1} in V, hat ein Urbild y_1 in L: Wir setzen y_1 gleich 0 in der offenen Menge $U \cup V_{f_1}$ und gleich $\tilde{x}_1^{-1}$ in der offenen Menge U_{f_1}. Das Element $\tilde{z}_1 = \widetilde{x_1 y_1}$ aus $\tilde{H}$ nimmt auf U_{f_1} den Wert 1 und sonst in V den Wert Null an. Mit endlich vielen offenen Mengen U_{f_ϱ}, $\varrho = 1, \ldots, n$, die wir disjunkt annehmen dürfen, überdecken wir V. Das Element $\tilde{u} = \tilde{z}_1 + \cdots + \tilde{z}_n$ liegt dann in $\tilde{H}$. — Unsere Annahme hat also zu einem Widerspruch geführt, d. h. es gibt ein Element f in $M(L)$, so daß $f(x) = 0$ ist für alle $x \in H$; dann ist $H = (x \text{ aus } L\colon f(x) = 0)$.

Mit unserer Voraussetzung, daß $M(L)$ trennt, können wir in $L(T)$ eine auf $M(L)$ bezogene neue Topologie einführen: $\mathbf{N} = (N_j)$, mit $j \in J$, bezeichne alle Mengen N_j von Elementen aus $M(L)$, von welchen für jedes feste x nur endlich viele einen von 0 verschiedenen Wert aus K annehmen. Da die Vereinigung endlich vieler Mengen N_j wieder zu $\mathbf{N}$ gehört und alle endlichen Mengen in $\mathbf{N}$ liegen, erklären die Orthogonalräume $N_j^\perp$ auf L eine Topologie, welche wir die *F-Topologie* T_F von L nennen wollen. Nach § 1, (7) ist $L(T_F)$ eine lineartopologische Algebra, denn die Mengen $N_j^\perp$ sind Ideale in L. Die Topologie T_F ist feiner als die durch ω_d in L^* induzierte Topologie T_i, in welcher gerade alle Elemente aus $M(L)$ stetig sind; genauer ergibt sich:

(11) *Eine Nullumgebungsbasis der F-Topologie ist durch alle solchen Durchschnitte D von T_i-offenen Idealen gegeben, deren Restklassenalgebra L^*/D isomorph einer Algebra φ_d ist.*

Beweis. Sei L^*/D (algebraisch) isomorph φ_d; dann ist $D^\perp \cap M(L)$ eine Menge N_j, denn sonst tritt wegen (1) in φ_d ein Element mit unendlich vielen von Null verschiedenen Komponenten auf. Es ist $N_j^\perp = D$. — Andererseits ist für eine Menge $N_j^\perp$ gewiß $L^*/N_j^\perp$ eine Subalgebra S von φ_d, wo d die Mächtigkeit von N_j bedeutet. Ist $x \in S$ und sind die Komponenten x_i und x_k nicht gleich 0, so können wir stets ein Element y in S finden, für welches $y_i \neq 0$ ist, während y_k verschwindet, und welches außerdem Nullkomponenten hat überall, wo die entsprechende Komponente von x verschwindet: Sei $x_i = rx_k$. Man sieht sofort, daß rf für $f \in M^-(L)$ und $r \neq 1$ nicht in $M^-(L)$ liegen kann. Deshalb sind zwei Projektionen p_i und p_k in S nicht proportional, d. h. es gibt ein Element z in S mit $z_i \neq rz_k$. Ist $z_k = 0$, so muß also $z_i \neq 0$ sein, und wir setzen $y = zx$. Wenn $z_k \neq 0$ ist und $z_i = 0$, so setzen wir $y = x - \frac{1}{z_k} zx$. Sind schließlich z_i und z_k beide von Null verschieden, sei etwa $z_i = sz_k$, so dürfen wir noch $s \neq 1$ annehmen; für $r = 1$ gilt dies nach Wahl von z; wenn $r \neq 1$ ist, kann für z das Element x^2 genommen werden. Hier setzen wir ebenfalls $y = x - \frac{1}{z_k} zx$. Dann ist in allen drei Fällen y ein Element von S mit den gewünschten Eigenschaften. — Fortführung dieser Konstruktion zeigt, daß der Einheitsvektor e_i in S liegt, d. h. es ist $S = \varphi_d$.

(12) *Wenn $M^-(L)$ diskret ist, dann stimmt die F-Topologie überein mit der Topologie T_k der uniformen Konvergenz auf allen kompakten Teilmengen von $M(L)$.*

Beweis. Sei N_k eine kompakte Teilmenge von $M(L)$. Für eine Nullumgebung U in $M(L)$ ist dann das Komplement von $U \cap N_k$ in N_k diskret und kompakt, d. h. endlich. Also ist N_k eine Menge N_j aus $\mathbf{N}$, denn für ein Element x aus L ist $x^\perp$ eine solche Nullumgebung U. Nimmt man umgekehrt die Nullabbildung Θ zu einer Menge N_j aus $\mathbf{N}$ hinzu, so ist $V = N_j \cup \Theta$ kompakt: Wenn U eine Umgebung von Θ in V ist, so können wir U als $(x_1, \ldots, x^k)^\perp \cap V$ annehmen, wo x_i Elemente aus L sind. In $(x_1, \ldots, x_n)^\perp$ liegen aber nach Definition von N_j alle Elemente von N_j bis auf endlich viele. Das Komplement von U in V ist also endlich und V besitzt die Heine-Borelsche Überdeckungseigenschaft. — Die Mengen $N_j^\perp = (N_j \cup \Theta)^\perp$ erklären die F-Topologie und die Mengen $N_k^\perp$ die Topologie der uniformen Konvergenz in den kompakten Teilmengen von $M(L)$ (vgl. Beweis von

§ 1, Satz 7). Hier ist C_L an die Stelle von L gesetzt. Damit ist unsere Behauptung bewiesen.

Wir wollen an einem Beispiel zeigen, daß $M^-(L)$ nicht immer diskret ist, selbst dann nicht, wenn $L(T)$ eine volle lineartopologische Algebra ist:

Die Menge E bestehe aus den Punkten 0, 2 und allen Punkten $\frac{1}{n}$, $2-\frac{1}{n}$, für $n=1,2,\ldots$ der reellen Zahlengeraden Z; dabei sei E mit der durch Z induzierten Topologie T' versehen. Die Algebra $L = C_0(E)$ enthält Funktionen, welche für alle Elemente ξ aus E verschwinden, die kleiner sind als ein bestimmtes Element $\frac{1}{n_0}$, und welche einen konstanten Wert haben für alle ξ, die größer sind als etwa $2-\frac{1}{n_1}$. Die Zuordnung $x \to (x_\xi) = (x(\xi))$ mit $x \in L$, sowie $\xi \in E$ und x_ξ ein Element des Grundkörpers K (= reelle Zahlen mit der diskreten Topologie), bildet L isomorph ab auf eine Subalgebra L^{**} von ω_d, wo d die Mächtigkeit von E^- (= E ohne 0) angibt. Mit H_ξ bezeichnen wir das Ideal aller auf $\xi \in E$ verschwindenden Elemente von L^{**}. Wir bilden die zu allen H_ξ gehörige Topologie T und erhalten eine lineartopologische Algebra $L^{**}(T)$ (vgl. § 1, (7)); die Topologie T ist gleich der durch ω_d in L^{**} induzierten Topologie T_i. Setzen wir $\xi(x) = x(\xi)$, so liegen die Elemente ξ von E in $M(L^{**})$. Sei nun h eine nichttriviale homomorphe Abbildung von $L^{**}(T)$ auf K. Wir wollen nachweisen, daß h in E liegt. In L^{**} liegen die Vektoren e^η mit den Komponenten

$$p_\xi(e^\eta) = \begin{cases} 0 & \text{für } \xi \neq \eta \\ 1 & \text{für } \xi = \eta \end{cases},$$

wo η alle Elemente von E durchläuft mit Ausnahme von 0 und 2 und p_ξ die Projektion auf die ξ-te Komponente in L^{**} bedeutet. Wenn h ein Element e^{η_0} in 1 überführt, so ist $h = p_{\eta_0}$ (vgl. Beweis von (4)), d. h. gleich η_0, und unsere Behauptung ist richtig. Im anderen Fall ist $h(e^\eta) = 0$ für alle η. Dann sei x ein beliebiges, nun festgehaltenes Element aus L^{**} und $2(x) = a$. Den Wert a nimmt x in einer ganzen Umgebung U von 2 an. Mit $\mathfrak{e}_x$ kennzeichnen wir das Element von L^{**}, das in einer offenen und abgeschlossenen Umgebung $V < U$ von 2 den Wert 1 hat und sonst auf E verschwindet. Die von $\mathfrak{e}_x$ und allen e^η aufgespannte Subalgebra S von $L^{**}(T)$ ist ersichtlich dicht in $L^{**}(T)$. Da $h^{(-1)}(0)$ in $L^{**}(T)$ abgeschlossen ist und nach unserer Annahme $h(e^\eta) = 0$ ist für alle η, ist notwendig $h(\mathfrak{e}_x) \neq 0$, d. h. $h(\mathfrak{e}_x) = 1$, denn $\mathfrak{e}_x$ ist idempotent. Es folgt $h(x) = h(x\mathfrak{e}_x) = h(a\mathfrak{e}_x) = a$, also $h(x) = 2(x)$. Für jedes x stimmt demnach h mit der durch das Element 2 auf $L^{**}(T)$ erzeugten Abbildung überein. Deshalb enthält E alle homomorphen Abbildungen von $L^{**}(T)$ in K.

Die schwache Topologie $T_s(L)$ auf E wird erzeugt von allen Mengen $x^{(-1)}(r)$, wo x in L liegt und r in K; da alle Elemente von L stetig sind in $E(T')$, ist $x^{(-1)}(0)$ offen bezüglich T', d. h. T_s ist gröber als T'. Auch in $E(T_s)$ ist jeder Punkt $\xi \neq \begin{cases} 0 \\ 2 \end{cases}$ isoliert, denn die T_s-offene Menge $(e^\xi)^{(-1)}(1)$ enthält nur ξ. Sei nun U eine beliebige Umgebung von 2 in $E(T')$, die wir offen und abgeschlossen annehmen dürfen. Erkläre ich eine Abbildung g von E in K durch die Festsetzung

$$g(\xi) = \begin{cases} 1 & \text{auf } U \\ 0 & \text{sonst} \end{cases},$$

so ist g stetig in $E(T')$, d. h. g liegt in L; es ist $U = g^{(-1)}(1)$. Folglich ist auch jede T'-Umgebung von 2 und ebenso von 0 eine T_s-Umgebung dieses Elementes; deshalb ist $T_s(L) = T'$ und $E(T') = M(L)$ (wie immer mit der schwachen Topologie versehen).

$L(T)$ ist also eine volle lineartopologische Algebra und $M^-(L)$ ist nicht diskret, sondern besitzt den Häufungspunkt 2.

Im Gegensatz zu den Verhältnissen bei der schwachen Topologie (§ 2, (9)) erhalten wir hier:

(13) *Die F-Topologie kann streng feiner und streng gröber sein als die Ausgangstopologie.*

Denn die diskrete Topologie T' auf ω ist streng feiner als die übliche Produkttopologie T. Setzen wir voraus, daß K wenigstens abzählbar ist, so haben ω und $\omega(T')$ nach (3) dasselbe $M(L)$. Die F-Topologie für $\omega(T')$ ist die Topologie T, da $\mathbf{N}$ in diesem Fall offenbar nur endliche Mengen enthält; sie ist also streng gröber als die Ausgangstopologie T'. — Ein Beispiel für die andere Aussage ist φ mit der durch ω induzierten Topologie T_i. Diese Topologie ist streng gröber als die übliche diskrete Topologie auf φ, welche die F-Topologie von $\varphi(T_i)$ ist ($\mathbf{N}$ enthält jetzt $M(L)$).

Die in der F-Topologie vollständigen lineartopologischen Algebren $L(T)$ lassen sich genauer beschreiben. Wir nennen eine Menge P_j von Koordinaten in L^* eine *P-Menge*, wenn alle Elemente x von L^* auf P_j nur endlich viele von Null verschiedene Koordinaten haben; wir sagen: x ist *finit auf P_j*. Die zu den Koordinaten aus P_j gehörenden Projektionen bilden eine Menge N_j aus $\mathbf{N}$. Enthält L^* alle auf seinen P-Mengen finiten Elemente aus ω_d, so wollen wir $L(T)$ eine *vollkommene lineartopologische Algebra* nennen. Es gilt nun:

Satz 5. *Genau dann ist $L(T)$ vollkommen, wenn L vollständig ist in der F-Topologie.*

Beweis. a) Sei das Element y aus ω_d finit auf allen P-Mengen P_j, mit $j \in J$, von L^*. Wenn $N_j^\perp$ das Ideal aller Elemente x aus L^* bezeichnet, welche Nullkomponenten auf P_j haben, so ist $L^*/N_j^\perp$ nach (11) isomorph der Algebra φ_c, wo c die Mächtigkeit von P_j ist. Deshalb gibt es zu jedem Index $j \in J$ ein Element y^j in L^*, welches auf P_j dieselben Koordinaten hat wie y. Weil die Vereinigung endlich vieler P-Mengen wieder eine P-Menge ist, bilden alle Mengen $y^j + N_j^\perp$ eine Basis eines Cauchyfilters G für die F-Topologie. G konvergiert nach Voraussetzung gegen ein Element z aus L^*. Alle Mannigfaltigkeiten $y^j + N_j^\perp$ sind F-abgeschlossen, enthalten also den Berührungspunkt z; d. h. z hat dieselben Komponenten wie y.

b) Jeder F-Cauchyfilter G enthält einen gröberen Filter G_1 mit Subbasis $(y^j + N_j^\perp)$, mit $j \in J$, wo y^j als Element von L^* nur endlich viele Nichtnullen auf P_j hat. Das Element x aus ω_d habe auf P_j dieselben Komponenten wie y^j für alle $j \in J$; ein solches Element gibt es, weil G_1 ein Filter ist. Dann gehört x zu L^*, weil dieses Element finit ist auf allen P-Mengen, und x ist ersichtlich Limes des Filters G_1 in der F-Topologie.

Korollar. *Wenn eine lineartopologische Algebra $L(T)$ mit trennendem $M(L)$ vollständig ist bezüglich einer Topologie, welche gröber ist als die F-Topologie und feiner als die durch ω_d in L^* induzierte Topologie T_i, so ist $L(T)$ vollkommen.*

Denn man benötigt offenbar nur, daß der Filter mit Basis $(y^j + N_j^\perp)$ ein Cauchyfilter ist, und daß alle Mengen $y^j + N_j^\perp$ abgeschlossen sind.

Die vollkommenen Algebren gehören zur Klasse der oben betrachteten vollen Algebren:

(14) *Eine vollkommene Algebra $L(T)$ ist voll.*

Beweis. $C_0(M(L))$ ist isomorph einer Subalgebra L^{**} von ω_d, wo d die Mächtigkeit von $M^-(L)$ angibt, durch die Zuordnung $x \to (x_i) = (x(f_i))$, mit $x \in C_0(M(L))$, wo f_i über $M^-(L)$ läuft. Die Algebra L^* ist in L^{**} enthalten als Bild von C_L bei der Abbildung von $C_0(M(L))$ auf L^{**}. Nach Definition der Mengen N_j aus $\mathbf{N}$ umfaßt andererseits der Durchschnitt einer Nullumgebung in $M(L)$ mit einer Menge N_j alle Elemente aus N_j bis auf

endlich viele Ausnahmen; denn für $y \in L$ enthält $y^{\perp}$ alle Elemente einer Menge N_j bis auf endlich viele und jede Nullumgebung in $M(L)$ umfaßt den Durchschnitt endlich vieler solcher Mengen $y^{\perp}$. Deshalb nimmt ein Element z aus $C_0(M(L))$ nur auf endlich vielen Elementen aus N_j einen von Null verschiedenen Wert an, d. h. (z_i) ist finit auf P_j und liegt also in L^*.

Bei einer vollkommenen Algebra $L(T)$ ist $M^-(L)$ stets diskret, denn L^* enthält nach Definition den Einheitsvektor e_i und in der in L' offenen Menge $e_i^{(-1)}(1)$ liegt von $M^-(L)$ nur die Projektion p_i. Demnach ist eine vollkommene Algebra, als Menge der in Θ verschwindenden stetigen Abbildungen von $M(L)$ in K betrachtet, vollständig bezüglich der Topologie T_k der uniformen Konvergenz in allen kompakten Teilmengen von $M(L)$ (vgl. (12) und Satz 5). Ob man auf der anderen Seite bei einer vollen lineartopologischen Algebra $L(T)$ aus Vollständigkeit bezüglich der kompakten Konvergenz T_k ohne die Voraussetzung „$M^-(L)$ diskret" schließen kann, daß $L(T)$ vollkommen ist, weiß ich nicht zu sagen.

Gehen wir nun umgekehrt von einem separierten, topologischen Raum E mit Topologie T und Elementen f_i, mit $i \in I$, aus; ein Element f_0 in E sei dadurch ausgezeichnet, daß das Komplement E^- von f_0 in E diskret ist. L bedeute die Algebra aller stetigen Abbildungen x von E in K, welche für f_0 verschwinden, wobei Summe und Produkt in L punktweise erklärt seien. Mit der Festsetzung $f_i(x) = x(f_i)$, für alle $x \in L$, kann man dann jedes Element f_i aus E als homomorphe Abbildung von L in K betrachten und E ist wegen der Bedeutung der Elemente von L eine trennende Menge homomorpher Abbildungen von L auf K. Es gilt:

(15) *Ist L vollständig bezüglich der Topologie T' der uniformen Konvergenz auf allen kompakten Teilmengen M_k von $E(T)$, so ist $E(T) = M(L)$, d. h. auch $T = T_s(L)$, und die Algebra $L(T')$ ist vollkommen.*

Beweis. L ist wie unter (14) isomorph abbildbar auf eine Subalgebra L^{**} von ω_d, wo d die Mächtigkeit von E^- ist. $L^{**}(T')$ ist nach § 1, Satz 7, eine idealtopologische Algebra, und eine Nullumgebungsbasis bilden die Ideale $M_k^{\perp}$. Ist U eine Umgebung von f_0 in E, so ist das Komplement V von $U \cap M_k$ in M_k abgeschlossen, d. h. kompakt und diskret nach Voraussetzung; also ist V endlich. Für ein Element x aus L ist $x^{(-1)}(0)$ eine offene Umgebung von f_0, d. h. x verschwindet auf allen Punkten von M_k mit Ausnahme von endlich vielen; daher hat das x in L^{**} entsprechende Element $(x_i) = (x(f_i))$ modulo $M_k^{\perp}$ nur endlich viele von Null verschiedene Komponenten. Weil E^- diskret ist, gehören die Einheitsvektoren e_i zu L^{**}; unsere Überlegung zeigt, daß die von allen e_i erzeugte Subalgebra S von L^{**} in $L^{**}(T')$ dicht ist. Wenn nun h eine nichttriviale, stetige, homomorphe Abbildung von $L^{**}(T')$ bzw. $L(T')$ auf K ist, so kann h nicht alle e_i in Null überführen; denn $h^{(-1)}(0)$ ist abgeschlossen und S ist dicht in $L^{**}(T')$. Ist aber $h(e_j) \neq 0$, so folgt $h = f_j$ (vgl. Beweis von (4)). Da $f_i^{\perp}$ in $L(T')$ offen ist, ist umgekehrt jedes Element aus E eine stetige, homomorphe Abbildung von $L(T')$ in K, d. h. E besteht gerade aus allen stetigen, homomorphen Abbildungen von $L(T')$ in K. Wie in dem Gegenbeispiel im Anschluß an (12) ist die schwache Topologie $T_s(L)$ auf E gröber als T, und auch in T_s ist E^- diskret. Sei nun U eine beliebige offene Umgebung von f_0 in $E(T)$; dann ist das Komplement W von U in E eine T-offene Menge, denn jedes Element aus W ist isoliert in $E(T)$. Erkläre ich demnach eine Abbildung y von E in K durch die Festsetzungen $y(U) = 0$ und $y(W) = 1$, so ist y stetig bzgl. T, also ist $y \in L$ und $U = y^{(-1)}(0)$. Dies zeigt, daß auch jede T-Umgebung von f_0 eine T_s-Umgebung dieses Elementes ist; deshalb ist $T_s(L) = T$ und demnach $E(T) = M(L)$. Die Algebra L^{**} ist die Algebra L^* aus Satz 1 und T' gleich der Topologie T_k aus (12), d. h. gleich der F-Topologie. Satz 5 vollendet den Beweis unserer Behauptung.

Betrachten wir wieder einen separierten topologischen Raum E mit Topologie T' und die Algebra $L = C_0(E)$ aller für ein festes Element ξ_0 aus E verschwindenden stetigen Abbildungen von $E(T')$ auf einen diskreten Körper K. Wir versehen L mit der durch die Ideale $H_\xi = (x \in L\colon x(\xi) = 0)$ erklärten Topologie T; dann ist $L(T)$ nach § 1, (7) eine idealtopologische Algebra. Im Zusammenhang mit (15) und dem Gegenbeispiel nach (12) interessiert nun, unter welchen Voraussetzungen $M(L)$ homöomorph $E(T')$ ist. Es gilt:

(16) *Genau dann ist $M(L) = E(T')$, wenn in $E(T')$ jeder Punkt eine Umgebungsbasis aus zugleich offenen und abgeschlossenen Mengen besitzt.*

Beweis. In $L'(T_s(L))$ ist die Bedingung erfüllt, also auch in $M(L)$. Es ist deshalb nur noch zu zeigen, daß sie hinreicht. Wir bilden L wie unter (15) wieder auf L^{**} ab, eine Subalgebra von ω_d, wo d die Mächtigkeit des Komplementes E^- von ξ_0 in E ist; auf L^{**} ist T ersichtlich gleich der durch ω_d induzierten Topologie T_i und $L^{**}(T)$ ist dicht in ω_d: Sei ein Element u von ω_d vorgegeben und eine Umgebung U von u durch die (endlich vielen) Komponenten $u_{\xi_1}, \ldots, u_{\xi_n}$ gekennzeichnet. Es gibt paarweise disjunkte Umgebungen $V_1, \ldots, V_n$ von $\xi_1, \ldots, \xi_n$ in $E(T')$, welche wir offen und abgeschlossen annehmen können und welche ξ_0 nicht enthalten. Erklären wir eine Abbildung g von $E(T')$ in K durch die Festsetzungen

$$g(\xi) = \begin{cases} u_{\xi_i} \text{ für } \xi \in V_i,\ i = 1, \ldots, n, \\ 0 \text{ sonst}, \end{cases}$$

so ist g stetig in $E(T')$ und g verschwindet in ξ_0, d. h. g liegt in $L(T)$. Also gibt es in L^{**} ein (g entsprechendes) Element y mit $y_{\xi_i} = u_{\xi_i}$ für $i = 1, \ldots, n$; dieses Element y gehört demnach zu U und $L^{**}(T)$ ist dicht in ω_d.

Wenn nun h eine beliebige homomorphe, stetige Abbildung von $L^{**}(T)$ auf K ist, so läßt sich h stetig auf ganz ω_d fortsetzen. Auf ω_d ist h nach (3) eine Projektion, darum stimmt h auf L^{**} mit einer Projektion, d. h. mit einem $\xi \in E$ überein. Alle Elemente aus $E(T')$ erklären umgekehrt stetige, homomorphe Abbildungen von $L(T)$ in K; also besteht $E(T')$ gerade aus allen stetigen, homomorphen Abbildungen von $L(T)$ auf K.

Wieder ist (wie im oben erwähnten Gegenbeispiel) die schwache Topologie $T_s(L)$ auf E gröber als die Topologie T'. Sei V eine beliebige offene und abgeschlossene Umgebung eines Elementes $\xi \neq \xi_0$ von E und sei $\xi_0 \notin V$; dann erklären wir mit $f(\xi) = \begin{Bmatrix} 1 \text{ für } \xi \in V \\ 0 \text{ sonst} \end{Bmatrix}$ eine stetige Abbildung f von $E(T')$ in K, die in ξ_0 verschwindet; deshalb ist f ein Element von $L(T)$ und es ist $V = f^{(-1)}(1)$. Ist W eine abgeschlossene und offene Umgebung von ξ_0, so erhalten wir durch $g(\xi) = \begin{Bmatrix} 0 \text{ für } \xi \in W \\ 1 \text{ sonst} \end{Bmatrix}$ ein Element aus L und es ist $W = g^{(-1)}(0)$. Die T'-Umgebungen V und W sind demnach auch offen in $T_s(L)$, d. h. die schwache Topologie stimmt mit T' überein und es ist also $E(T) = M(L)$.

Wir wollen unsere Überlegungen zu einer Kennzeichnung der lineartopologischen Algebren ω_d und φ_d benutzen.

(17) *Bei trennendem $M(L)$ sind die folgenden Eigenschaften einer lineartopologischen Algebra $L(T)$ äquivalent und sie bedingen, daß $L(T)$ topologisch isomorph ist (bezüglich der jeweils angegebenen Topologie) zu ω_d, wo d die Mächtigkeit von $M^-(L)$ angibt:*

1. *L ist schwach vollständig;*
2. *L ist vollständig bezüglich der schwächsten Topologie T', in welcher alle Elemente f aus $M(L)$ stetig sind;*

3. *$L(T)$ ist linear kompakt;*
4. *$L(T_s)$ ist voll und $M(L)$ diskret;*
5. *$L(T)$ ist voll und $C_0(M(L))$ vollständig bezüglich der Topologie T'' der einfachen Konvergenz.*

Beweis. 1. entspricht 3. nach § 2, Satz 2, Korollar. Im Fall 2. ist $L(T')$ nach § 1, Satz 2, eine lineartopologische Algebra mit einer Nullumgebungssubbasis aus Subalgebren mit endlichem Defekt, d. h. wegen § 2, (11) ist $T' = T_s$, so daß 1. und 2. gleichbedeutend sind. Für 2. gilt die Behauptung nach § 2, (11), § 2, Satz 4 und § 2, (20). In 4. ist L isomorph ω_d über die Zuordnung $x \longleftrightarrow (x_i)$, mit $x_i = x(f_i)$, wo f_i in $M^-(L)$ variiert. Die Komponenten x_i eines Elementes können dabei beliebig vorgegebene Werte aus K annehmen, da $M(L)$ diskret, also jede Abbildung x von $M(L)$ in K stetig ist. Dieselbe Zuordnung zeigt, daß L unter der Voraussetzung 5. isomorph abbildbar ist auf eine Subalgebra S von ω_d, und die Topologie T'' ist ersichtlich die durch ω_d in S induzierte Topologie; hier ist die Aussage nach dem Beweis von (16) richtig. Daß in allen Fällen die angegebene Topologie (in 5. die Topologie T'') die in ω_d übliche Produkttopologie ist, ist klar.

Für φ_d erhalten wir:

(18) *Eine lineartopologische Algebra $L(T)$ habe ein trennendes $M(L)$ und die Mächtigkeit von $M^-(L)$ sei d. Genau dann ist die Algebra L^* (aus Satz 1) gleich φ_d, wenn $M(L)$ kompakt ist und $M^-(L)$ diskret.*

Beweis. Nach dem Beweis von (5) enthält jede Nullumgebung in $M(\varphi_d)$ alle Elemente bis auf endlich viele, d. h. $M(\varphi_d)$ erfüllt die Heine-Borelsche Überdeckungsbedingung und ist also kompakt. $M^-(\varphi_d)$ ist diskret, da diese Menge gerade aus allen Projektionen p_i besteht und die Einheitsvektoren e_i in φ_d liegen; die offene Menge $e_i^{(-1)}(1)$ von $M(L)$ enthält nur p_i. Sind umgekehrt obige Eigenschaften vorausgesetzt, so ist das Komplement einer Nullumgebung in $M(L)$ kompakt und diskret, d. h. endlich; deshalb hat jedes Element von L^* als stetige Abbildung von $M(L)$ in K (wir identifizieren L^* mit C_L) unter seinen Komponenten nur endlich viele Nichtnullen, d. h. es gilt $L^* < \varphi_d$. Die Schlußweise aus (11) weist hier $L^* = \varphi_d$ nach.

Da $M(\varphi_d)$ trennt, ist die (in φ_d übliche) diskrete Topologie auf L^* als Topologie der uniformen Konvergenz auf $M(L)$ gekennzeichnet.

Ebenso folgt, daß eine volle lineartopologische Algebra $L(T)$ mit trennendem $M(L)$ algebraisch genau dann von der Form $\varphi_d + \omega_c$ ist, wenn $M(L)$ eine kompakte Nullumgebung U hat (d. h. lokal kompakt ist) und wenn jedes Element $f \neq \Theta$ aus $M(L)$ isoliert ist: Ist $L = \varphi_d + \omega_c$, so schreibt sich jedes Element x aus L als $x = (\xi_\nu; \eta_\mu)$, mit $(\xi_\nu) \in \varphi_d$ und $(\eta_\mu) \in \omega_c$. In dem Element y aus L seien alle Komponenten ξ_ν gleich 0, während alle η_μ den Wert 1 haben sollen. $y^\perp$ ist eine Nullumgebung U in $M(L)$ und das Komplement jeder anderen Nullumgebung in U ist endlich, da für ein x nur endlich viele ξ_ν nicht verschwinden. Also ist U (wie oben $(M\varphi_d)$) kompakt. Ein Element $f \neq \Theta$ aus $M(L)$ ist isoliert, weil die Einheitsvektoren e_i in L liegen (ein ξ_ν oder ein η_μ hat in e_i den Wert 1, alle anderen Komponenten sind 0). — Ist auf der anderen Seite $M^-(L)$ diskret und U eine kompakte Nullumgebung in $M(L)$, so ist das Komplement jeder Nullumgebung in U kompakt und diskret, also endlich. Ein Element x aus L nimmt demnach, als stetige Abbildung auf $M(L)$ betrachtet, nur auf endlich vielen Elementen aus U einen von Null verschiedenen Wert an. Hingegen kann x auf dem Komplement W von U in $M(L)$ beliebig vorgegebene Werte aus K annehmen; denn dieses Komplement ist diskret und offen. Also ist $x = (\xi_\nu; \eta_\mu)$, wo ξ_ν die Bildpunkte von U bei der Abbildung x durchläuft und η_μ die Bildpunkte von W. Das Verfahren aus (11) zeigt wieder, daß (ξ_ν) ein beliebiges

Element aus φ_d, wo d die Mächtigkeit von U ist, sein kann; auch (η_μ) ist, wie schon gesagt, als Element von ω_c keiner Beschränkung unterworfen, wenn c die Mächtigkeit von W ist.

In (18) und auch im eben angegebenen Beispiel wirkt wieder die Bedingung „$M^-(L)$ diskret" störend. Es fragt sich, ob schon eine volle, lineartopologische Algebra $L(T)$ mit kompaktem $M(L)$ sich isomorph abbilden läßt auf φ_d, wo d die Mächtigkeit von $M^-(L)$ ist. Ich vermag diese Frage nicht zu entscheiden. Aus den Voraussetzungen schließt man sofort, daß nur endlich viele Skalare aus K unter den Komponenten eines Elementes x aus L^* auftreten. Aus dieser Eigenschaft kann man aber die gewünschte Isomorphie zu φ_d nicht direkt herleiten, wie das folgende Beispiel zeigt: Sei K der Körper der reellen Zahlen, mit der diskreten Topologie versehen. L bedeute die Menge aller Elemente aus ω, deren Komponentenfolge periodisch ist, z. B. $x = (1231231\ldots)$. Die Menge L ist dann abgeschlossen bezüglich Summen- und Produktbildung, weil hierdurch z. B. aus einem Element mit einer n-gliedrigen und einem anderen mit einer m-gliedrigen Periode eines entsteht, das gewiß eine nm-gliedrige Periode besitzt. L ist also eine Algebra; als Komponenten eines festen Elementes x aus L treten nur endlich viele verschiedene Skalare aus K auf, aber L enthält die Einheitsvektoren e_i nicht.

Literaturverzeichnis.

I. *N. Bourbaki*, Topologie générale, chap. I, II. Actual. sci. industr. 858 = 1142, Paris 1951.

II. *N. Bourbaki*, Topologie générale, chap. X. Actual. sci. industr. 1084, Paris 1949.

III. *Jean Dieudonné*, Linearly compact spaces and double vector spaces over sfields. Amer. J. Math. **73**, 13—19 (1951).

IV. *Einar Hille*, Functional analysis and semi-groups, Amer. Math. Soc. Colloquium Publications **31**, New York 1948.

V. *N. Jacobson*, The radical and semi-simplicity in arbitrary rings. Amer. J. Math. **67**, 300—320 (1945).

VI. *Irving Kaplansky*, Topological rings. Amer. J. Math. **69**, 153—183 (1947).

VII. *Irving Kaplansky*, Locally compact rings. Amer. J. Math. **70**, 447—459 (1948).

VIII. *Gottfried Köthe*, Topologische lineare Räume. Erscheint demnächst in der Sammlung: Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen. Die Textverweise beziehen sich stets auf Kapitel II.

IX. *G. Köthe* und *O. Toeplitz*, Lineare Räume mit unendlich vielen Koordinaten und Ringe unendlicher Matrizen. J. reine angew. Math. **171**, 193—226 (1934).

X. *Solomon Lefschetz*, Algebraic topology. Amer. Math. Soc. Colloquium Publications **27**, New York 1942.

XI. *Ernest Michael*, Locally multiplicatively-convex topological algebras. Memoirs of the Amer. Math. Soc. **11**, New York 1952.

XII. *B. L. van der Waerden*, Moderne Algebra II. Grundl. math. Wissensch. **34**, 2. Auflage. Berlin 1940.

XIII. *André Weil*, L'intégration dans les groupes topologiques et ses applications. Actual. sci. industr. 869, Paris 1940.

XIV. *Daniel Zelinsky*, Linearly compact modules and rings. Amer. J. Math. **75**, 79—90 (1953).

XV. *Daniel Zelinsky*, Rings with ideal nuclei. Duke math. J. **18**, 431—442 (1951).

Eingegangen 9. Februar 1954.

Dualität in der Funktionentheorie auf Riemannschen Flächen.

Von *Heinz Günther Tillmann*, z. Zt. Ibadan (Nigeria).

Einleitung.

Im Anschluß an eine Arbeit von J. S. e Silva[1]) wurden von G. Köthe[2]) und A. Grothendieck[3]) gewisse Räume von analytischen bzw. lokalanalytischen Funktionen in schlichten Bereichen untersucht. Es ergab sich eine Integraldarstellung der stetigen linearen Funktionale und der stetigen linearen Abbildungen, wodurch den Abbildungen umkehrbar eindeutig gewisse analytische (bzw. lokalanalytische) Funktionen mit Vektorwerten zugeordnet werden.

In der vorliegenden Arbeit werden nun lineare Räume von analytischen Funktionen auf Riemannschen Flächen betrachtet. Als Definitionsbereiche werden an Stelle schlichter Punktmengen beliebige Bereiche auf einer beliebigen Riemannschen Fläche $\mathfrak{R}$ zugelassen.

Es sei $\mathfrak{M}$ eine Punktmenge der Riemannschen Fläche $\mathfrak{R}$. Wir betrachten lokalanalytische Funktionen in $\mathfrak{M}$. Dabei heißt eine Funktion $f(p)$ *lokalanalytisch* in $\mathfrak{M}$, wenn $f(p)$ in einer offenen Menge $\mathfrak{U} > \mathfrak{M}$ eindeutig und in jeder Komponente von $\mathfrak{U}$ analytisch ist. Zwei Funktionen, die in ihren Funktionselementen in den Punkten von $\mathfrak{M}$ übereinstimmen, werden als nicht voneinander verschieden angesehen.

Mit $\mathfrak{H}(\mathfrak{M})$ bezeichnen wir den Raum aller in $\mathfrak{M}$ lokalanalytischen Funktionen.

Im Hinblick auf die stetigen linearen Abbildungen von $\mathfrak{H}(\mathfrak{M})$ in einen Vektorraum E ist es zweckmäßig, auch analytische Funktionen mit Werten in einen Vektorraum E heranzuziehen. $\mathfrak{H}(\mathfrak{M}, E)$ sei also der Raum aller in $\mathfrak{M}$ lokalanalytischen Funktionen mit Werten in dem topologischen Vektorraum E.

Ist K der Körper der komplexen Zahlen, so gilt also $\mathfrak{H}(\mathfrak{M}) = \mathfrak{H}(\mathfrak{M}, K)$. In $\mathfrak{H}(\mathfrak{M}, E)$ führen wir nun eine Topologie $\mathfrak{T}_2$ ein, die mit der gleichmäßigen Konvergenz verknüpft ist. Für offene Mengen $\mathfrak{O}$ ist die Topologie $\mathfrak{T}_2$ in $\mathfrak{H}(\mathfrak{O}, E)$ genau die Topologie der gleichmäßigen Konvergenz im Innern von $\mathfrak{O}$.

Da die Arbeiten von G. Köthe und A. Grothendieck sich entscheidend auf die Cauchysche Integralformel stützen, werden wir natürlich die von H. Behnke und K. Stein[4]) gewonnene Übertragung dieser Formel für nichtschlichte Gebiete benutzen.

In § 1 bringen wir dann neben einer Zusammenstellung der Eigenschaften analytischer Funktionen mit Vektorwerten diese Formel für Funktionen, deren Werte einem Vektorraum E angehören (Satz 1). Entscheidend ist dabei die von H. Behnke und K. Stein[4]) bewiesene Existenz einer komplexwertigen *Elementarfunktion* 1. *Ordnung* $A(p, q)$ zu jeder offenen Riemannschen Fläche $\mathfrak{R}'$.

---

[1]) *J. S. e Silva* [7] (Literaturverzeichnis am Ende der Arbeit).
[2]) *G. Köthe* [4], [5].
[3]) *A. Grothendieck* [3].
[4]) *H. Behnke-K. Stein* [1].

Der § 2 ist der Definition der Räume $\mathfrak{H}(\mathfrak{M}, E)$ und ihrer Topologie sowie der Untersuchung einiger topologischer Eigenschaften dieser Räume gewidmet. Nach diesen Vorbereitungen können in § 3 die stetigen linearen Funktionale auf $\mathfrak{H}(\mathfrak{M}, E)$ bestimmt werden. Jedem stetigen linearen Funktional $u[f]$ auf $\mathfrak{H}(\mathfrak{M}, E)$ läßt sich umkehrbar eindeutig eine in $\mathbf{C}\mathfrak{M} = \mathfrak{R} - \mathfrak{M}$ lokalanalytische Funktion $u'(q)$ mit Werten aus dem zu E dualen Raum E' zuordnen:

$$u'(q)\,[x] = \langle x, u'(q)\rangle = {}_{D/}\, u_p[x \cdot A(p, q)].$$

Die $u'(q)$ sind in bezug auf q lokal gleichgradig stetige lineare Funktionale auf E. Weiterhin ist $u'(q)$ *bianalytisch*, d. h. $u'(q)$ ist analytisch im Komplement einer kompakten Menge $\mathfrak{K}$ und für jede Umgebung $\mathfrak{U}(\mathfrak{K})$ gilt:

$$u'(q) = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{U}(\mathfrak{K})} A(q, p)\, u'(p)\, dp\,^{5)}.$$

Der zu $\mathfrak{H}(\mathfrak{M}, E)$ duale Raum ist also isomorph zu dem Raum $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$ der in $\mathbf{C}\mathfrak{M}$ bianalytischen Funktionen mit Werten aus E' (Satz 9) die lokal gleichgradig stetig sind[6]). In $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$ wird auch eine Topologie $\mathfrak{T}'_2$ der gleichmäßigen Konvergenz definiert und gezeigt: Die Topologie $\mathfrak{T}'_2$ in $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M})$ stimmt mit der starken Topologie $\mathfrak{T}_b$ der gleichmäßigen Konvergenz auf den beschränkten Mengen von $\mathfrak{H}(\mathfrak{M})$ überein, und $\mathfrak{H}(\mathfrak{M})$ ist zu $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M})$ dual (Satz 11). Die Übereinstimmung von $\mathfrak{T}'_2$ und $\mathfrak{T}_b$ in $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$ konnte weiterhin gezeigt werden, wenn $\mathfrak{M}$ offen und E totalreflexiv ist.

Für beliebige $\mathfrak{M}$ konnte nur gezeigt werden, daß $\mathfrak{T}'_2$ gröber ist als $\mathfrak{T}_b$. Ob die beiden Topologien übereinstimmen, bleibt noch offen.

§ 4 ist der Untersuchung der stetigen linearen Abbildungen der Räume $\mathfrak{H}(\mathfrak{M}, E)$ in einen lokalkonvexen Vektorraum F gewidmet. Wir geben die Resultate zur Vereinfachung nur für den Fall an, daß F vollständig ist.

Die einfachsten Verhältnisse liegen vor, wenn $\mathfrak{M} = \mathfrak{K}$ eine kompakte, echte Teilmenge von $\mathfrak{R}$ ist. Es gilt dann (Satz 13):

Der Raum $\mathfrak{L}(\mathfrak{H}(\mathfrak{K}, E), F)$ der stetigen linearen Abbildungen von $\mathfrak{H}(\mathfrak{K}, E)$ in F ist isomorph dem Raum $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{K}, \mathfrak{L}_b(E, F))$ der in $\mathbf{C}\mathfrak{K}$ bianalytischen Funktionen mit Werten aus dem Raum $\mathfrak{L}_b(E, F)$, wobei die Werte lokal gleichgradig stetige lineare Abbildungen von E in F sind. Die Isomorphie $T \leftrightarrow \widetilde{T}(q)$ wird geliefert durch $\widetilde{T}(q)[x] = T[x \cdot A(p, q)]$, x beliebig aus E, und es ist

$$T[f] = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{U}(\mathfrak{K})} \widetilde{T}(p)\,[f(p)]\, d\underline{p}.$$

Bei beliebigem $\mathfrak{M}$ können i. a. nicht mehr alle stetigen, wohl aber alle beschränkten Abbildungen von $\mathfrak{H}(\mathfrak{M}, E)$ in F auf diese Weise dargestellt werden (Satz 14).

Alle stetigen linearen Abbildungen erhält man, wenn man für $\widetilde{T}$ lokalanalytische Funktionen im weiteren Sinne[7]) zuläßt. Der Raum $\mathfrak{L}(\mathfrak{H}(\mathfrak{M}, E), F)$ ist isomorph zum Raum $\widetilde{\mathfrak{H}}^0_A(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$ der in $\mathbf{C}\mathfrak{M}$ lokal bianalytischen Funktionen i. w. S., deren

---

[5]) Ist $\mathfrak{G}$ ein Gebiet, daß $\mathfrak{K}$ und q enthält, so gilt also

$$\int\limits_{\mathrm{Rd}\,\mathfrak{G}} A(q, p)\, u'(p)\, d\underline{p} = 0.$$

[6]) Eine Funktion $f(p)$, deren Werte lineare Abbildungen eines Raumes E in einen Raum F sind, heißen *lokal gleichgradig stetig*, wenn es zu jedem p_0 aus dem Definitionsbereich von f eine Umgebung $\mathfrak{U}(p_0)$ gibt, so daß alle $f(p)$ für $p \in \mathfrak{U}(p_0)$ gleichgradig stetige lineare Abbildungen von E in F sind.

[7]) Abgekürzt: lokalanalytische Funktion i. w. S. (vgl. Def. 8).

Werte lokal gleichgradig stetige lineare Abbildungen von E in F sind. Besonders wichtig ist der Spezialfall $E = K$. Der Raum $\mathfrak{L}(\mathfrak{H}(\mathfrak{M}), F)$ ist isomorph zum Raum $\tilde{\mathfrak{H}}_A^0(\complement\mathfrak{M}, F)$ der in $\complement\mathfrak{M}$ bianalytischen Funktionen i. w. S. mit Werten aus F.

Wir benutzen folgende Begriffe und Bezeichnungen:

$\mathfrak{R}$ ist stets eine Riemannsche Fläche, und Teilmengen von $\mathfrak{R}$ werden durch große Frakturbuchstaben bezeichnet.

Für die mengentheoretischen Operationen der Vereinigung und Durchschnittsbildung verwenden wir die üblichen Symbole $\smile$, $\cup$ und $\frown$, $\cap$ (z. B. $\mathfrak{G}_1 \smile \mathfrak{G}_2$; $\bigcap_{i=1}^{\infty} \mathfrak{G}_i$), und $\complement\mathfrak{M}$ ist das Komplement der Teilmenge $\mathfrak{M} < \mathfrak{R}$.

Die Inklusion $\mathfrak{M}_1 < \mathfrak{M}_2$ ist stets so zu verstehen, daß die Gleichheit von $\mathfrak{M}_1$ und $\mathfrak{M}_2$ eingeschlossen ist. $\mathfrak{M}_1 << \mathfrak{M}_2$ bedeutet, daß $\mathfrak{M}_1$ relativ kompakt in $\mathfrak{M}_2$ ist und auch die abgeschlossene Hülle $\overline{\mathfrak{M}}_1$ von $\mathfrak{M}_1$ noch im Innern von $\mathfrak{M}_2$ enthalten ist. Ist $\mathfrak{M}_1 < \mathfrak{M}_2$, so nennen wir $\mathfrak{M}_1$ relativ zu $\mathfrak{M}_2$ einfach zusammenhängend, wenn jedes Gebiet aus $\mathfrak{M}_2$, dessen Rand in $\mathfrak{M}_1$ liegt, ganz zu $\mathfrak{M}_1$ gehört.

Lineare Räume von analytischen Funktionen und Teilmengen solcher Räume werden durch große, fettgedruckte Frakturbuchstaben bezeichnet und $\Gamma_{i \in I} \mathfrak{U}_i$ ist die konvexe Hülle der Mengen $\mathfrak{U}_i$. Eine konvexe Menge V aus einem Vektorraum heißt *kreiskonvex*, wenn V durch die Drehungen $x \to e^{i\varphi} \cdot x$ $(0 \leqq \varphi \leqq 2\pi)$ in sich abgebildet wird. Diese Bedingung ist äquivalent damit, daß mit $x, y \in V$ auch $\alpha x + \beta y$ zu V gehört, wenn $|\alpha| + |\beta| \leqq 1$ ist. Eine Menge B aus einem topologischen Vektorraum E heißt *beschränkt*, wenn es zu jeder Umgebung $V < E$ ein $\lambda > 0$ gibt, so daß $B < \lambda V$ ist. $\langle x, x' \rangle$ ist das skalare Produkt eines Elementes $x \in E$ und eines Funktionals x' aus dem zu E dualen Raume E', und $\mathfrak{L}(E, F)$ ist der Raum aller stetigen linearen Abbildungen von E in F. Falls er mit der Topologie der gleichmäßigen Konvergenz auf allen beschränkten Mengen aus E versehen ist, schreiben wir auch $\mathfrak{L}_b(E, F)$.

§ 1. Analytische Funktionen mit Werten in topologischen Vektorräumen.

Es sei E ein lokalkonvexer, separierter, topologischer Vektorraum über dem Körper K der komplexen Zahlen. Die Topologie $\mathfrak{T}_E$ von E wird erzeugt durch ein System $\mathfrak{B} = \{V\}$ von kreiskonvexen Umgebungen. Jeder solchen Umgebung V entspricht eine Halbnorm $N_V(x)$ in E mit der Eigenschaft:

$$x \in \overline{V} \leftrightarrow N_V(x) \leqq 1. \tag{1}$$

Die Topologie $\mathfrak{T}_E$ kann also auch durch das System $\Gamma = \{N_V\}_{V \in \mathfrak{B}}$ von Halbnormen definiert werden. Die Separiertheit des Raumes entspricht der Bedingung, daß nur für $x = 0$ alle definierenden Halbnormen verschwinden.

Kann die Topologie $\mathfrak{T}_E$ durch eine einzige Norm erzeugt werden, so ist E Banachraum (B-Raum) und bei abzählbar vielen definierenden Halbnormen ist E ein Fréchetraum (F-Raum), sofern E vollständig ist.

Definition 1. *$f(z)$ sei eine Abbildung des Gebietes $\mathfrak{D}$ der komplexen Zahlenebene in den topologischen Vektorraum E. $f(z)$ heißt in $\mathfrak{D}$ analytisch, wenn für jedes stetige lineare Funktional x' auf E (also $x' \in E'$) die Funktion $x'[f(z)] = \langle f(z), x' \rangle$ eine komplexwertige analytische Funktion in $\mathfrak{D}$ ist.*

Es gilt [8]: $f(z)$ ist dann und nur dann analytisch, wenn

a) $f(z)$ schwach stetig ist und der Cauchysche Integralsatz $\int_C f(z)\,dz = 0$ gilt.

b) $f(z)$ schwach stetig ist und die Cauchysche Integralformel $f(z) = \frac{1}{2\pi i}\int_C \frac{f(\zeta)}{\zeta - z}\,d\zeta$ erfüllt (hieraus folgt sogar, daß $f(z)$ stark stetig ist).

Hinreichend ist die folgende Bedingung:

c) $f(z)$ ist schwach differenzierbar.

Falls E halbvollständig ist, ist diese Bedingung auch notwendig. Dann ist $f(z)$ sogar beliebig oft stark differenzierbar und es gilt:

d) $$f^{(n)}(z) = \frac{n!}{2\pi i}\int_C \frac{f(\zeta)\,d\zeta}{(\zeta - z)^{n+1}}$$

und die Taylorentwicklung

e) $$f(z+h) = \sum_0^\infty \frac{f^{(n)}(z)}{n!}\,h^n,$$

wobei die Reihe in einer Umgebung $|h| \leqq r$ im Sinne der Topologie von E gleichmäßig konvergiert.

In der Umgebung einer isolierten Singularität z_0 gilt die Laurententwicklung

f) $$f(z_0 + h) = \sum_{-\infty}^{+\infty} a_n h^n \quad \text{mit} \quad a_n = \frac{1}{2\pi i}\int_C \frac{f(\zeta)\,d\zeta}{(\zeta - z)^{n+1}},$$

also auch der Residuensatz

$$\int_{\Gamma = \mathrm{Rd}\,\overline{\mathfrak{G}}} f(z)\,dz = \sum_{z_i \in \mathfrak{G}} \mathrm{Res}\,(f, z_i).$$

Ferner gilt das Maximumprinzip in der folgenden Formulierung:

g) Sei $\mathfrak{G}$ einfach zusammenhängend, $\Gamma = \mathrm{Rd}\,\mathfrak{G}$ und $f(z)$ in $\mathfrak{G}$ analytisch und in $\mathfrak{G} \cap \Gamma$ stetig. Ist B eine kreiskonvexe, abgeschlossene Menge in E, die die Funktionswerte von f für $z \in \Gamma$ enthält, so enthält B auch alle Werte von f für $z \in \mathfrak{G}$.

Die Laurententwicklung ergibt sich aus der Taylorentwicklung wie bei komplexwertigen Funktionen. Das Maximumprinzip (g) erhält man durch konforme Abbildung von $\mathfrak{G}$ auf die Einheitskreisscheibe und Anwendung der Cauchyschen Integralformel.

Funktionen auf Riemannschen Flächen. Um die analytischen Funktionen mit Vektorwerten in ihrem Gesamtverlauf als eindeutige Funktionen behandeln zu können, muß man sie natürlich auch als Funktionen auf Riemannschen Flächen auffassen [9].

Es sei nun $\mathfrak{R}$ eine konkrete Riemannsche Fläche, d. h. jedem Punkte $p \in \mathfrak{R}$ sei eine komplexe Zahl oder ∞ als Grundpunkt $z = \underline{p}$ zugeordnet ($p = p(z)$). Ist $p_0(z_0)$ bzw. $p_0(\infty)$ ein beliebiger Punkt von $\mathfrak{R}$ und ist die Verzweigungsordnung in p_0 gleich $\nu - 1$, so wird eine eineindeutige Abbildung einer Umgebung von p_0 auf eine schlichte Umgebung des Nullpunktes der komplexen t-Ebene gegeben durch:

(2) $$\underline{p}(z) - \underline{p}(z_0) = z - z_0 = t^\nu \quad \text{bzw.} \quad \frac{1}{\underline{p}(z)} = \frac{1}{z} = t^\nu$$

(t = ausgezeichnete Ortsuniformisierende).

---

[8]) Vgl. *A. Grothendieck* [3], Theorème I.

[9]) Als Existenzgebiet der Funktion $f(p)$ erhält man die *Riemann*sche Fläche, auf die alle die komplexwertigen Funktionen $\langle f(p), x'\rangle$, $x' \in E'$, gleichzeitig fortsetzbar sind.

Eine Funktion $f(p)$, die in einem Gebiet $\mathfrak{D} < \mathfrak{R}$ definiert ist, kann also lokal als Funktion einer Ortsuniformisierenden aufgefaßt werden:

$$f(p) = f(p(t)) = \tilde{f}(t). \tag{3}$$

Definition 2. *Eine Funktion $f(p)$ mit Werten aus dem topologischen Vektorraum E heiße in dem Gebiet $\mathfrak{D} < \mathfrak{R}$ analytisch, wenn für alle Stellen $p_0 \in \mathfrak{D}$ eine Umgebung $\mathfrak{U}(p_0)$ existiert, derart, daß für alle $p \in \mathfrak{U}(p_0)$ die Funktionen $f(p) = f(p(t))$ als Funktion der zu p_0 gehörigen Ortsuniformisierenden t analytisch ist.*

Definition 3. *Ist $f(p)$ in einer Umgebung von p_0 außer in p_0 selbst analytisch, so versteht man unter dem Residuum von $f(p)$ im Punkte p_0 den Koeffizienten von $\frac{1}{t}$ in der Laurententwicklung der Funktion $\tilde{f}(t) = f(p(t)) \frac{\partial p(t)}{\partial t}$ nach einer Ortsuniformisierenden t in p_0.*

Das Residuum hängt von der Wahl der Ortsuniformisierenden nicht ab, sondern ist durch $f(p)$ und p_0 allein bestimmt.

Durch Zerlegung in Elementargebiete überträgt man nun den Residuensatz auf Funktionen auf Riemannschen Flächen.

Residuensatz. *Es sei C eine endliche rektifizierbare Kurve, die ein Gebiet $\mathfrak{G} << \mathfrak{R}$ berandet. $f(p)$ sei in $\mathfrak{G}$ mit Ausnahme von höchstens endlich vielen Stellen $p_1, \ldots, p_k$ analytisch und auf $\mathfrak{G} \cup C$ noch stetig. Dann ist*

$$\frac{1}{2\pi i}\int_C f(p)\,dp = \frac{1}{2\pi i}\int_C f(p(z))\,dz = \sum_{j=1}^{k} \operatorname{Res}(f(p), p_i). \tag{4}$$

Für $k = 0$ ergibt sich der Cauchysche Integralsatz:

$$\frac{1}{2\pi i}\int_C f(p)\,dp = \frac{1}{2\pi i}\int_C f(p(z))\,dz = 0. \tag{5}$$

Die Übertragung der Cauchyschen Integralformeln ist jedoch nicht ohne weiteres möglich. Dazu ist es erforderlich, einen Ersatz für den Cauchykern $\frac{1}{\xi - z}$ zu finden.

Definition 4. *Sei $\mathfrak{R}'$ eine nichtgeschlossene Riemannsche Fläche. Eine komplexwertige Funktion $A(p, q)$ heiße Elementarfunktion 1. Ordnung auf $\mathfrak{R}'$, wenn folgendes gilt:*

1. *$A(p, q)$ verhält sich in $\mathfrak{R}'_p \times \mathfrak{R}'_q$ meromorph.*
2. *$A(p, q)$ ist für $p \neq q$ (q als Parameter) analytisch.*
3. *$A(p, q)$ hat für $p = q$ einen einfachen Pol mit dem Residuum $+1$.*

Ist also t eine Ortsuniformisierende in p_0, τ eine Ortsuniformisierende in q_0, so gestattet $A(p(t), q(\tau)) \frac{\partial p}{\partial t}$ in der Umgebung von (p_0, q_0) die Entwicklung

$$A(p(t), q(\tau)) \frac{\partial p(t)}{\partial t} = R(t, \tau) \qquad \text{für } p_0 \neq q_0,$$

$$A(p(t), q(\tau)) \frac{\partial p(t)}{\partial t} = \frac{1}{t - \tau} + S(t, \tau) \quad \text{für } p_0 = q_0,$$

wobei $R(t, \tau)$ und $s(t, \tau)$ analytisch in t und τ sind.

H. Behnke und K. Stein[10]) haben nun gezeigt, daß es zu jeder nichtgeschlossenen Riemannschen Fläche $\mathfrak{R}'$ solche Elementarfunktionen gibt. $A(p, q)$ ist natürlich nicht eindeutig bestimmt, da man zu $A(p, q)$ noch beliebige auf $\mathfrak{R}'_p \times \mathfrak{R}'_q$ analytische Funktionen addieren kann.

Unter Benutzung einer solchen Elementarfunktion läßt sich nun die Cauchysche Integralformel auch für Funktionen auf $\mathfrak{R}'$ mit Vektorwerten übertragen[11]).

Satz 1. *Sei $\mathfrak{G}$ ein echtes Teilgebiet der Riemannschen Fläche $\mathfrak{R}$ und C der Rand von $\mathfrak{G}$. Die Spurkurve $\underline{C}$ von C sei rektifizierbar und $A(p, q)$ sei eine Elementarfunktion 1. Ordnung auf einer Riemannschen Fläche $\mathfrak{R}' < \mathfrak{R}$, die $\mathfrak{G} \cup C$ ganz im Innern enthält. Dann ist für jede in $\mathfrak{G}$ analytische und in $\mathfrak{G} \cup C$ stetige Funktion $f(p)$ mit Werten in E:*

$$f(p) = \frac{1}{2\pi i} \int_C f(q)\, A(q, p)\, dq \quad \text{für alle } p \in \mathfrak{G}. \tag{6}$$

Die Riemannschen Summen $\frac{1}{2\pi i} \sum_{q_\nu \in C} f(q_\nu)\, A(q_\nu, p)\, \Delta q_\nu$ konvergieren in jedem kompakten Teilgebiet von $\mathfrak{G}$ gleichmäßig gegen $f(p)$ im Sinne der Topologie von E.

Beweis. Ist $\mathfrak{G}$ ein relativ kompaktes Teilgebiet von $\mathfrak{R}$ mit dem Rande C, so gibt es stets eine offene Riemannsche Fläche $\mathfrak{R}' < \mathfrak{R}$ die $\mathfrak{G} \cup C$ im Innern enthält ($\mathfrak{R}'$ kann z. B. durch Herausnahme eines nicht zu $\mathfrak{G} \cup C = \overline{\mathfrak{G}}$ gehörigen Punktes aus $\mathfrak{R}$ gewonnen werden). Aus dem Residuensatz folgt dann aber unmittelbar:

$$f(p) = \frac{1}{2\pi i} \int_C f(q)\, A(q, p)\, dq = \operatorname{Res}\big(f(q) \cdot A(q, p), p\big).$$

Sei nun $\mathfrak{K}$ ein kompaktes Teilgebiet von $\mathfrak{G}$. Die Funktion $A(q, p)$ ist in $C_q \times \mathfrak{K}_p$ analytisch, also beschränkt durch eine Konstante M. Man kann die Kurve C durch endlich viele Elementargebiete $\mathfrak{G}_1, \ldots, \mathfrak{G}_k$ überdecken und jedes dieser Gebiete $\mathfrak{G}_i$ durch eine Ortsuniformisierende $t_i = t_i(q)$ auf eine schlichte Umgebung des Nullpunktes abbilden. In $(\mathfrak{G}_i \cap C)_q \times \mathfrak{K}_p$ ist $A(q, p)$ gleichmäßig stetig in t_i und p. Zu jedem $\varepsilon > 0$ gibt es ein $\delta > 0$, so daß aus $|t_i(q) - t_i(q')| \leqq \delta$ stets $|A(q, p) - A(q', p)| \leqq \varepsilon$ folgt für alle $p \in \mathfrak{K}$. Da $f(q)$ auf C stetig ist, kann man δ auch so klein wählen, daß für eine beliebige kreiskonvexe Umgebung $V < E$

$$f(q) - f(q') \in V, \quad \text{falls } |t_i(q) - t_i(q')| \leqq \delta.$$

Sei nun $\mathfrak{Z} = \{q_0, q_1, \ldots, q_e = q_0\}$ eine Zerlegung der Kurve C, die so fein sei, daß $|t_i(q_j) - t_i(q^*_{j+1})| \leqq \delta$[12]) ist für alle Punkte q^*_{j+1} auf C, die zwischen q_j und q_{j+1} liegen. Dann gilt für eine Verfeinerung

$$\mathfrak{Z}' = \{q_0 = q_{00}, q_{01}, \ldots, q_1 = q_{10}, \ldots, q_e = q_0\}$$

die Relation

$$\sum_{\mathfrak{Z}} f(q_\nu)\, A(q_\nu, p)\, \Delta q_\nu - \sum_{\mathfrak{Z}'} f(q_{\nu\mu})\, A(q_{\nu\mu}, p)\, \Delta q_{\nu\mu}$$
$$= \sum_{\mathfrak{Z}'} \{(f(q_\nu) - f(q_{\nu\mu}))\, A(q_\nu, p) + f(q_{\nu\mu})\, (A(q_\nu, p) - A(q_{\nu\mu}, p))\}\, \Delta q_{\nu\mu} \in (V \cdot M + B \cdot \varepsilon) \sum |\Delta q_{\nu\mu}|,$$

---

[10]) Vgl. *H. Behnke-K. Stein* [1].

[11]) Für komplexwertige Funktionen wurde dies von *H. Behnke-K. Stein* (a. a. O. [10])) durchgeführt.

[12]) Man kann ja offenbar voraussetzen, daß die Zerlegung $\mathfrak{Z}$ so fein ist, daß je zwei aufeinanderfolgende Teilpunkte q_j, q_{j+1} und alle Punkte q^*_{j+1} auf C zwischen q_j und q_{j+1} in einem Elementargebiet $\mathfrak{G}_i = g_{i(j)}$ liegen, so daß also $t_i(q_j)$, $t_i(q_{j+1})$ und $t_i(q^*_{j+1})$ definiert sind.

wo B eine beschränkte, kreiskonvexe Menge in E ist, die die Funktionswerte $f(q)$ für $q \in C$ enthält. Ist nun U eine beliebige kreiskonvexe Umgebung in E, so wählt man $V = \frac{\pi}{M \cdot \int_C |dq|} U$ und ε so klein, daß $\varepsilon B < \frac{\pi}{\int |dq|} U$ ist. Dann gilt also

$$\frac{1}{2\pi i} \sum_{\mathfrak{Z}} f(q_\nu) A(q_\nu, p) \Delta q_\nu - \frac{1}{2\pi i} \sum_{\mathfrak{Z}'} f(q_{\nu\mu}) A(q_{\nu\mu}, p) \Delta q_{\nu\mu} \in \frac{\Sigma |\Delta q_{\nu\mu}|}{\int |dq|} U < U \text{ für alle } p \in \mathfrak{K}.$$

Die Riemannschen Summen $\frac{1}{2\pi i} \Sigma f(q_\nu) A(q_\nu, p) \Delta q_\nu$ konvergieren also mit $\delta \to 0$ gleichmäßig für alle $p \in \mathfrak{K}$ gegen $f(p)$ im Sinne der Topologie $\mathfrak{T}_E$ von E, w. z. b. w.

§ 2. Lineare Räume von Funktionen auf Riemannschen Flächen.

Es sei $\mathfrak{M}$ eine beliebige Teilmenge der Riemannschen Fläche $\mathfrak{K}$.

Definition 5. *Eine Funktion $f(p)$ mit Werten in dem Vektorraum E soll lokalanalytisch in $\mathfrak{M}$ heißen, wenn $f(p)$ in einer Umgebung $\mathfrak{U}$ von $\mathfrak{M}$ eindeutig definiert und in jeder Komponente von $\mathfrak{U}$ analytisch ist. Dabei soll zwischen Funktionen, die auf einer Umgebung von $\mathfrak{M}$ übereinstimmen, nicht unterschieden werden.*

Ist $\mathfrak{M}$ ein Gebiet, so ist also eine in $\mathfrak{M}$ lokalanalytische Funktion nichts anderes als eine in $\mathfrak{M}$ analytische Funktion. Ist $\mathfrak{M}$ beliebig, so ist eine lokalanalytische Funktion $f(p)$ nicht notwendig durch ihre Werte auf $\mathfrak{M}$, wohl aber durch ihre Funktionselemente in den Punkten von $\mathfrak{M}$ festgelegt.

Die Gesamtheit der lokalanalytischen Funktionen in $\mathfrak{M}$ mit Werten aus E bezeichnen wir mit $\mathfrak{H}(\mathfrak{M}, E)$. Falls $E = K$ (Körper der komplexen Zahlen) ist, schreiben wir auch einfach $\mathfrak{H}(\mathfrak{M})$ für $\mathfrak{H}(\mathfrak{M}, K)$. In den Räumen $\mathfrak{H}(\mathfrak{M}, E)$ führen wir nun geeignete Topologien ein, die mit der gleichmäßigen Konvergenz verknüpft sind. Zur Definition der Topologie in $\mathfrak{H}(\mathfrak{M}, E)$ benutzen wir Räume des folgenden Typs:

I. Die Räume $\mathfrak{B}(\mathfrak{U}, E)$. Es sei $\mathfrak{U}$ eine offene, relativ kompakte Teilmenge von $\mathfrak{K}$ und $\overline{\mathfrak{U}}$ die abgeschlossene Hülle von $\mathfrak{U}$.

$\mathfrak{B}(\mathfrak{U}, E)$ sei die Gesamtheit der in $\mathfrak{U}$ analytischen und in $\overline{\mathfrak{U}}$ stetigen Funktionen mit der Topologie $\mathfrak{T}_0$ der gleichmäßigen Konvergenz in $\overline{\mathfrak{U}}$. Diese Topologie $\mathfrak{T}_0$ wird definiert durch die Umgebungen

$$\mathfrak{U}_0(\mathfrak{U}, V) = \{f(p);\ f \in \mathfrak{B}(\mathfrak{U}, E) \wedge (p \in \overline{\mathfrak{U}} \to f(p) \in V)\}, \tag{7}$$

wobei V ein fundamentales Umgebungssystem $\mathfrak{V}$ von E durchläuft.

Satz 2. *Der Raum $\mathfrak{B}(\mathfrak{U}, E)$ ist dann und nur dann vollständig (bzw. normierbar bzw. metrisierbar), wenn der Raum E vollständig (bzw. normierbar bezw. metrisierbar) ist.*

Beweis. Der abgeschlossene Teilraum der konstanten Funktionen aus $\mathfrak{B}(\mathfrak{U}, E)$ ist zu E topologisch isomorph. Damit ist die Vollständigkeit (bzw. Normierbarkeit bzw. Metrisierbarkeit) von E für die entsprechende Eigenschaft von $\mathfrak{B}(\mathfrak{U}, E)$ notwendig.

Sei nun E vollständig und $\Phi = \{\mathfrak{F}\}$ ein Cauchyfilter in $\mathfrak{B}(\mathfrak{U}, E)$. Es sei $\mathfrak{F}_p = \{f(p)\}_{f \in \mathfrak{F}}$. Dann ist $\Phi_p = \{\mathfrak{F}_p\}$ für jeden Punkt $p \in \overline{\mathfrak{U}}$ ein Cauchyfilter in E, konvergiert also gegen einen Vektor $g_0(p) \in E$. Es ist g_0 also eine Funktion in $\overline{\mathfrak{U}}$ mit Werten aus E. Da Φ Cauchyfilter ist, konvergiert Φ aber sogar gleichmäßig gegen $g_0(p)$. Als Limes eines gleichmäßig konvergenten Filters analytischer Funktionen ist aber $g_0(p)$ in $\mathfrak{U}$ analytisch und auf $\overline{\mathfrak{U}}$ noch stetig, gehört also zu $\mathfrak{B}(\mathfrak{U}, E)$.

Jeder Halbnorm $\| x \|$ in E ist eindeutig die Halbnorm $|||f||| = \sup_{p \in \bar{\mathfrak{U}}} \| f(p) \|$ zugeordnet und für konstante Funktionen $f(p) = x$ reduziert sich $|||f|||$ auf $\| x \|$. Kann die Topologie in E also durch eine (bzw. abzählbar viele) Halbnormen definiert werden, so gilt das gleiche von $\mathfrak{T}_0$ in $\mathfrak{B}(\mathfrak{U}, E)$.

II. Die Räume $\mathfrak{H}(\mathfrak{D}, E)$ für offene Mengen $\mathfrak{D}$. Die Topologie $\mathfrak{T}_1$ in $\mathfrak{H}(\mathfrak{D}, E)$ sei die Topologie der gleichmäßigen Konvergenz im Innern von $\mathfrak{D}$. Wir können sie auf die folgende Weise definieren: Die offene Menge $\mathfrak{D}$ können wir normal ausschöpfen[13]) durch eine monotone Folge von Mengen $\mathfrak{G}_k$, die relativ kompakt in $\mathfrak{D}$ sind. Man kann voraussetzen, daß die $\mathfrak{G}_k$ aus je endlich vielen Komponenten endlichen Zusammenhanges mit rektifizierbaren Rändern bestehen und die Bedingung

$$\mathfrak{G}_1 \ll \mathfrak{G}_2 \ll \mathfrak{G}_3 \ll \cdots \ll \mathfrak{D}; \quad \mathfrak{D} = \bigcup_{k=1}^{\infty} \mathfrak{G}_k \tag{8}$$

erfüllen. Es ist dann offenbar

$$\mathfrak{H}(\mathfrak{D}, E) = \bigcap_{k=1}^{\infty} \mathfrak{B}(\mathfrak{G}_k, E), \tag{9}$$

und die Topologie $\mathfrak{T}_1$ ist die Durchschnittstopologie. Sie wird definiert durch die Gesamtheit der Umgebungen

$$\mathfrak{U}_1(\mathfrak{D}, \mathfrak{G}_k, V) = \{f;\ f \in \mathfrak{H}(\mathfrak{D}, E) \wedge (p \in \mathfrak{G}_k \to f(p) \in V\}. \tag{10}$$
$$k = 1, 2, \ldots;\ V \in \mathfrak{V}.$$

Satz 3. *Ist $\mathfrak{D}$ offen, so ist $\mathfrak{H}(\mathfrak{D}, E)$ dann und nur dann ein F-Raum (M-Raum), wenn E ein F-Raum (M-Raum) ist.*

Beweis. Wird die Topologie $\mathfrak{T}_E$ durch ein abzählbares Umgebungssystem $\mathfrak{V} = \{V_i\}$ definiert, so ist $\{\mathfrak{U}_1(\mathfrak{D}, \mathfrak{G}_h, V_i) = \mathfrak{U}_1(h, i)\}$ ein abzählbares Umgebungssystem in $\mathfrak{H}(\mathfrak{D}, E)$, dieser Raum ist also metrisierbar. Eine Cauchyfolge $\{f_i\}$ in $\mathfrak{H}(\mathfrak{D}, E)$ ist auf jeder kompakten Teilmenge von $\mathfrak{D}$ gleichmäßig konvergent. Wenn E vollständig ist, konvergiert $\{f_i\}$ also gegen eine in $\mathfrak{D}$ analytische Grenzfunktion mit Werten aus E. Der Raum $\mathfrak{H}(\mathfrak{D}, E)$ ist also auch vollständig.

Sei E ein M-Raum. Eine Menge $\mathfrak{B} \subset \mathfrak{H}(\mathfrak{D}, E)$ ist dann und nur dann beschränkt, wenn alle $f \in \mathfrak{B}$ auf jedem kompakten Teilgebiet von $\mathfrak{D}$ gleichmäßig beschränkt sind. Ist $p_1, p_2, \ldots p_m, \ldots$ eine abzählbare, in $\mathfrak{D}$ dichte Punktmenge, so kann man also aus $\mathfrak{B}$ eine Teilfolge $\{f_i\}$ auswählen, die in allen Punkten p_m konvergiert. Da die Funktionen aus $\mathfrak{B}$ in jedem Elementargebiet bezüglich einer Uniformisierenden gleichgradig stetig sind, konvergieren die f_i aber in jedem kompakten Teilgebiet $\mathfrak{K} \subset \mathfrak{D}$ sogar gleichmäßig gegen eine Funktion f_0, die dann notwendig zu $\mathfrak{H}(\mathfrak{D}, E)$ gehört.

Ist nämlich $\bar{\mathfrak{U}} = \bar{\mathfrak{U}}(p_0)$ eine Umgebung von p_0 in $\mathfrak{D}$, die durch die Ortsuniformisierende $t = t(p)$ auf den Einheitskreis abgebildet wird, so gilt für alle $f \in \mathfrak{B}$ für eine beschränkte kreiskonvexe, abgeschlossene Menge $B \subset E$:

$$f(p) \in B \text{ für alle } p \in \bar{\mathfrak{U}}(p_0).$$

Für $p_1 \in \mathfrak{U}(p_0)$ gilt nun die Cauchysche Formel

$$f(p_1(t_1)) = \frac{1}{2\pi i} \int_{|t|=1} \frac{f(q(t))}{t - t_1}\, dt,$$

also

$$f(p_1(t_1)) - f(p_2(t_2)) = \frac{1}{2\pi i} \int_{|t|=1} f(q(t))\, \{(t - t_1)^{-1} - (t - t_2)^{-1}\}\, dt.$$

[13]) Eine zweite offene Menge $\mathfrak{G} \subset \mathfrak{D}$ heißt relativ zu $\mathfrak{D}$ *einfach zusammenhängend*, wenn jedes endliche System C von geschlossenen Kurven aus $\mathfrak{G}$, das in $\mathfrak{D}$ berandet (also vollständiger Rand einer Teilmenge von $\mathfrak{D}$ ist), auch bereits in $\mathfrak{G}$ berandet. Wir nennen eine Ausschöpfung von $\mathfrak{D}$ durch offene Mengen $\mathfrak{G}_k$ *normal*, wenn $\mathfrak{G}_{k-1} \ll \mathfrak{G}_k$ ist und wenn jedes $\mathfrak{G}_k$ relativ zu $\mathfrak{D}$ einfach zusammenhängend ist.

Ist nun V eine beliebige Umgebung in E, so gilt $B < \lambda V$ für genügend großes λ. Für $|t_i| \leqq \frac{1}{2}$, $|t_1 - t_2| \leqq \frac{4}{\lambda}$ gilt also:

$$f(p_1(t_1)) - f(p_2(t_2)) \in V \text{ für alle } f \in \mathfrak{B}.$$

In der Umgebung $\mathfrak{U}_1 = \{p;\ |t| \leqq \frac{1}{2} \wedge p = p(t)\}$ sind also die Funktionen aus $\mathfrak{B}$ gleichgradig stetig. Die Folge der Funktionen $f_i \in \mathfrak{B}$ konvergiert also nicht nur in den Punkten $p_1, \ldots, p_m, \ldots$, sondern in allen Punkten von $\mathfrak{D}$, und zwar ist die Konvergenz gleichmäßig in jedem kompakten Teilgebiet $\mathfrak{K} < \mathfrak{D}$, da $\mathfrak{K}$ durch endlich viele solcher Umgebungen $\mathfrak{U}_1$ überdeckt werden kann. Die f_i konvergieren also im Sinne der Topologie $\mathfrak{T}_1$ von $\mathfrak{H}(\mathfrak{D}, E)$ gegen f_0. Die beschränkte Menge $\mathfrak{B} < \mathfrak{H}(\mathfrak{D}, E)$ ist also relativ kompakt.

Aus dem Beweis geht zugleich hervor:

Ist in E jede beschränkte Menge relativ kompakt, so gilt das gleiche auch in $\mathfrak{H}(\mathfrak{D}, E)$, auch wenn E und damit $\mathfrak{H}(\mathfrak{D}, E)$ kein F-Raum ist.

Satz 4. *Es seien $\mathfrak{D}_1$, $\mathfrak{D}_2$ zwei offene Mengen und $\mathfrak{D}_1 < \mathfrak{D}_2$, ferner sei $\mathfrak{D}_1$ relativ zu $\mathfrak{D}_2$ einfach zusammenhängend. Dann ist $\mathfrak{H}(\mathfrak{D}_2, E)$ in $\mathfrak{H}(\mathfrak{D}_1, E)$ dicht.*

Beweis. Sei $\mathfrak{K}$ eine beliebige kompakte Teilmenge von $\mathfrak{D}_1$ und $\mathfrak{K} < \mathfrak{D} < \bar{\mathfrak{D}} < \mathfrak{D}_1$ und der Rand von $\mathfrak{D}$ rektifizierbar. Man kann $\mathfrak{D}$ so wählen, daß es relativ zu $\mathfrak{D}_1$ einfach zusammenhängend ist. In $\mathfrak{D}$ gilt nun für eine beliebige Funktion $f \in \mathfrak{H}(\mathfrak{D}_1, E)$

$$f(p) = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\bar{\mathfrak{D}}} f(q)\, A(q, p)\, dq = \lim \frac{1}{2\pi i} \sum f(q_\nu)\, A(q_\nu, p)\, \Delta q_\nu .$$

$A(q_\nu, p)$ ist eine analytische komplexwertige Funktion in $\mathfrak{D}$. Da $\mathfrak{D}$ relativ zu $\mathfrak{D}_2$ einfach zusammenhängend ist, läßt sich $A(q_\nu, p)$ nach einem Satz von H. Behnke-K. Stein[14]) im Innern von $\mathfrak{D}$, also insbesondere auf $\mathfrak{K}$, durch in $\mathfrak{D}_2$ analytische Funktionen $A_{\nu,\varepsilon}(p)$ gleichmäßig approximieren. Dann konvergieren die Funktionen

$$f_{\mathfrak{Z},\varepsilon}(p) = \frac{1}{2\pi i} \sum_{\mathfrak{Z}} f(q_\nu)\, A_{\nu,\varepsilon}(p)\, \Delta q_\nu \quad \text{für } \varepsilon \to 0 \text{ und } \Delta(\mathfrak{Z}) \to 0$$

auf $\mathfrak{K}$ gleichmäßig im Sinne der Topologie $\mathfrak{T}_E$ von E gegen $f(p)$. Der Raum $\mathfrak{H}(\mathfrak{D}_2, E)$ ist also in $\mathfrak{H}(\mathfrak{D}_1, E)$ dicht.

Satz 5. *Ist E_0 dicht in E, so ist $\mathfrak{H}(\mathfrak{D}, E_0)$ dicht in $\mathfrak{H}(\mathfrak{D}, E)$.*

Beweis. Für jede kompakte Teilmenge $\mathfrak{K}$ von $\mathfrak{D}$ gibt es eine in $\mathfrak{D}$ relativ kompakte und relativ einfach zusammenhängende offene Menge $\mathfrak{D}_0 > \mathfrak{K}$. Ist V eine beliebige Umgebung in E, so gibt es eine Zerlegung $\mathfrak{Z}$ des Randes von $\mathfrak{D}_0$, so daß für $p \in \mathfrak{K}$

$$f(p) - \frac{1}{2\pi i} \sum_{\mathfrak{Z}} f(q_\nu)\, A(q_\nu, p)\, \Delta q_\nu \in \frac{1}{3} V .$$

Da $\mathfrak{D}_0$ relativ zu $\mathfrak{D}$ einfach zusammenhängend ist, kann man $A(q_\nu, p)$ durch eine in $\mathfrak{D}$ analytische Funktion $A_{\nu,\varepsilon_\nu}(p)$ approximieren, so daß für $p \in \mathfrak{K}$

$$\frac{1}{2\pi i} \sum_{\mathfrak{Z}} f(q_\nu)\, A_{\nu,\varepsilon_\nu}(p)\, \Delta q_\nu - \frac{1}{2\pi i} \sum_{\mathfrak{Z}} f(q_\nu)\, A(q_\nu, p)\, \Delta q_\nu \in \frac{1}{3} V .$$

Da nun E_0 in E dicht ist, kann man noch die $f(q_\nu) \in E$ durch Vektoren f_ν aus E_0 ersetzen, so daß

$$\frac{1}{2\pi i} \sum \{f_\nu - f(q_\nu)\, A_{\nu,\varepsilon_\nu}(p)\, \Delta q_\nu \in \frac{1}{3} V$$

[14]) A. a. O. [1]).

ist. Insgesamt erhält man damit

$$f(p) - \frac{1}{2\pi i} \Sigma f_\nu A_{\nu,\varepsilon_\nu}(p)\, \Delta q_\nu \in V \text{ für alle } p \in \mathfrak{K};$$

also liegt $\frac{1}{2\pi i} \Sigma f_\nu A_{\nu,\varepsilon_\nu}(p)\, \Delta q_\nu \in \mathfrak{H}(\mathfrak{O}, E_0)$ in $f(p) + \mathfrak{U}_1(\mathfrak{O}, \mathfrak{K}, V)$. Da $\mathfrak{K}$ und V beliebig waren, liegt also $\mathfrak{H}(\mathfrak{O}, E_0)$ in $\mathfrak{H}(\mathfrak{O}, E)$ dicht, w. z. b. w.

Offenbar wird die Topologie $\mathfrak{T}_1$ in $\mathfrak{H}(\mathfrak{O}, E_0)$ von der Topologie $\mathfrak{T}_1$ in $\mathfrak{H}(\mathfrak{O}, E)$ induziert, wenn die Topologie in E_0 durch $\mathfrak{T}_E$ induziert ist.

Jedenfalls ist also eine stetige lineare Abbildung von $\mathfrak{H}(\mathfrak{O}, E)$ bereits durch ihre Werte auf $\mathfrak{H}(\mathfrak{O}, E_0)$ vollständig festgelegt.

III. Die Räume $\mathfrak{H}(\mathfrak{M}, E)$ für beliebiges $\mathfrak{M}$. Es sei $\mathfrak{S}(\mathfrak{M})$ das System aller offenen Mengen $\mathfrak{O} > \mathfrak{M}$, in denen jede zusammenhängende Komponente wenigstens einen Punkt von $\mathfrak{M}$ enthält. Dann ist offenbar

$$\mathfrak{M} = \bigcap_{\mathfrak{O} < \mathfrak{S}(\mathfrak{M})} \mathfrak{O}. \tag{11}$$

Da jede in $\mathfrak{M}$ lokalanalytische Funktion in einer ganzen Umgebung $\mathfrak{O} > \mathfrak{M}$ lokalanalytisch ist, gilt:

$$\mathfrak{H}(\mathfrak{M}, E) = \bigcup_{\mathfrak{O} \in \mathfrak{S}(\mathfrak{M})} \mathfrak{H}(\mathfrak{O}, E). \tag{12}$$

Die Topologie $\mathfrak{T}_2$ in $\mathfrak{H}(\mathfrak{M}, E)$ sei die Topologie der lokalkonvexen Hülle der Räume $\mathfrak{H}(\mathfrak{O}, E)$, d. h. die feinste lokalkonvexe Topologie, die auf jedem $\mathfrak{H}(\mathfrak{O}, E)$ eine Topologie induziert, die gröber als die Topologie $\mathfrak{T}_1$ von $\mathfrak{H}(\mathfrak{O}, E)$ ist. $\mathfrak{T}_2$ wird erzeugt durch die Umgebungen

$$\begin{aligned} \mathfrak{U}_2(\mathfrak{M}, \{\mathfrak{O}, \mathfrak{G}_\mathfrak{O}, V_\mathfrak{O}\}) &= \Gamma_{\mathfrak{O} \in \mathfrak{S}(\mathfrak{M})} \mathfrak{U}_1(\mathfrak{O}, \mathfrak{G}_\mathfrak{O}, V_\mathfrak{O}) \\ &= \left\{ f;\, f = \sum_1^m \alpha_i f_i \wedge \Sigma\, |\alpha_i| \leqq 1 \wedge f_i \in \mathfrak{U}_1(\mathfrak{O}_i, \mathfrak{G}_{\mathfrak{O}_i}, V_{\mathfrak{O}_i}) \right\}. \end{aligned} \tag{13}$$

Falls $\mathfrak{M}$ offen, also $\mathfrak{M} \in \mathfrak{S}(\mathfrak{M})$ ist, gilt:

$$\mathfrak{U}_1(\mathfrak{M}, \mathfrak{G}_\mathfrak{M}, V_\mathfrak{M}) < \mathfrak{U}_2(\mathfrak{M}, \{\mathfrak{O}, \mathfrak{G}_\mathfrak{O}, V_\mathfrak{O}\}), \quad \mathfrak{U}_2(\mathfrak{M}\{\mathfrak{O}, \mathfrak{G}_\mathfrak{M}, V_\mathfrak{M}\}) < \mathfrak{U}_1(\mathfrak{M}, \mathfrak{G}_\mathfrak{M}, V_\mathfrak{M}).$$

Dann stimmt also die Topologie $\mathfrak{T}_2$ mit $\mathfrak{T}_1$ überein.

Ist $\mathfrak{M}$ abgeschlossen, so gibt es bereits eine abzählbare monotone Folge von Mengen $\mathfrak{O}_i \in \mathfrak{S}(\mathfrak{M})$, deren Durchschnitt gleich $\mathfrak{M}$ ist. Da jede Menge $\mathfrak{O} \in \mathfrak{S}(\mathfrak{M})$ dann eine der Mengen $\mathfrak{O}_i$ enthält, ist auch $\mathfrak{H}(\mathfrak{M}, E) = \bigcup_{i=1}^{\infty} \mathfrak{H}(\mathfrak{O}_i, E) = \bigcup_{i=1}^{\infty} \mathfrak{B}(\mathfrak{O}_i, E)$.

Die Mengen

$$\tilde{\mathfrak{U}}_2(\mathfrak{M}, \{\mathfrak{O}_i, \mathfrak{G}_i, V_i\}) = \Gamma_{i=1}^{\infty} \mathfrak{U}_0(\mathfrak{G}_i, V_i) \frown \mathfrak{H}(\mathfrak{M}, E) \tag{14}$$

bilden ein fundamentales Umgebungssystem der Topologie $\mathfrak{T}_2$ von $\mathfrak{H}(\mathfrak{M}, E)$.

Wir bestimmen nun die beschränkten Mengen des Raumes $\mathfrak{H}(\mathfrak{M}) = \mathfrak{H}(\mathfrak{M}, K)$.

Satz 6. *Ist $\mathfrak{M}$ eine kompakte Teilmenge der Riemannschen Fläche $\mathfrak{R}$, so gilt: Eine Menge $\mathfrak{B} < \mathfrak{H}(\mathfrak{M})$ ist dann und nur dann beschränkt, wenn alle Funktionen $f \in \mathfrak{B}$ in einer ganzen Umgebung $\mathfrak{O} > \mathfrak{M}$ analytisch und gleichmäßig beschränkt sind.*

Beweis. Nach Satz 2 ist mit K auch $\mathfrak{B}(\mathfrak{O}_i, K)$ ein Banachraum. $\mathfrak{H}(\mathfrak{M}, K)$ ist also die lokalkonvexe Hülle der Banachräume $\mathfrak{B}(\mathfrak{O}_i, K)$. Es sei $\mathfrak{B}_i$ die abgeschlossene Einheitskugel in $\mathfrak{B}(\mathfrak{O}_i, K)$, d. h. $\mathfrak{B}_i = \mathfrak{U}_0(\mathfrak{O}_i, |x| \leqq 1)$. Die Menge $\mathfrak{B}_i$ ist also beschränkt in dem M-Raum $\mathfrak{H}(\mathfrak{O}_i, K)$, also relativ kompakt in diesem Raum. Da die Topologie $\mathfrak{T}_0$

in $\mathfrak{B}(\mathfrak{O}_{i+1}, K)$ wegen $\overline{\mathfrak{O}}_{i+1} < \mathfrak{O}_i$ gröber ist als die Topologie von $\mathfrak{H}(\mathfrak{O}_i, K)$, ist $\mathfrak{B}_i$ dann erst recht relativ kompakt in $\mathfrak{B}(\mathfrak{O}_{i+1}, K)$. Nach einem Satz von J. S. e Silva[15]) folgt dann, daß eine Menge aus $\mathfrak{H}(\mathfrak{M}, K)$ dann und nur dann beschränkt ist, wenn sie in einem der Räume $\mathfrak{B}(\mathfrak{O}_i, K)$ enthalten und dort beschränkt ist.

Satz 7. *Ist $\mathfrak{M}$ eine beliebige Teilmenge der Riemannschen Fläche $\mathfrak{R}$, so gilt: Eine Menge $\mathfrak{B} < \mathfrak{H}(\mathfrak{M})$ ist dann und nur dann beschränkt, wenn alle Funktionen $f \in \mathfrak{B}$ in einer offenen Menge $\mathfrak{O} > \mathfrak{M}$ analytisch und auf jeder kompakten Teilmenge von $\mathfrak{O}$ gleichmäßig beschränkt sind.*

Beweis. Sei p ein beliebiger Punkt aus $\mathfrak{M}$ und $\mathfrak{N}_p$ die Gesamtheit aller Funktionen aus $\mathfrak{H}(\mathfrak{M})$, die in der Umgebung von p identisch verschwinden. Der Quotientenraum $\mathfrak{H}^{(\mathfrak{M})}/\mathfrak{N}_p$ ist dann enthalten in $\mathfrak{H}(\{p\})$ und die durch die Topologie von $\mathfrak{H}(\mathfrak{M})$ in $\mathfrak{H}^{(\mathfrak{M})}/\mathfrak{N}_p$ induzierte Topologie ist feiner als die Topologie von $\mathfrak{H}(\{p\})$.

Das Bild von $\mathfrak{B}$ bei der natürlichen Abbildung von $\mathfrak{H}(\mathfrak{M})$ auf $\mathfrak{H}^{(\mathfrak{M})}/\mathfrak{N}_p \leqq \mathfrak{H}(\{p\})$ ist also beschränkt in $\mathfrak{H}(\{p\})$. Ist f_p das Funktionselement von $f \in \mathfrak{B}$ im Punkte p, so sind nach Satz 6 alle f_p in einer Umgebung $\mathfrak{U}_p = \mathfrak{U}(p)$ analytisch und gleichmäßig beschränkt.

Es sei nun $\mathfrak{O} = \bigcup_{p \in \mathfrak{M}} \mathfrak{U}_p$. Dann ist $\mathfrak{O}$ eine offene Menge, die $\mathfrak{M}$ enthält, auf der alle $f \in \mathfrak{B}$ analytisch sind. Ist $\mathfrak{K}$ eine kompakte Teilmenge von $\mathfrak{O}$, so wird $\mathfrak{K}$ bereits durch endlich viele Umgebungen $\mathfrak{U}_{p_1}, \ldots, \mathfrak{U}_{p_m}$ überdeckt. Da die Funktionen $f \in \mathfrak{B}$ in jedem $\mathfrak{U}_{p_i}$ gleichmäßig beschränkt sind, sind sie auch auf $\mathfrak{K} < \bigcup_1^m \mathfrak{U}_{p_i}$ gleichmäßig beschränkt, w. z. b. w.

Satz 5'. *Ist E_0 dicht in E, so ist $\mathfrak{H}(\mathfrak{M}, E_0)$ dicht in $\mathfrak{H}(\mathfrak{M}, E)$ für jede Menge $\mathfrak{M} < \mathfrak{R}$.*

Beweis. Sei $f(p) \in \mathfrak{H}(\mathfrak{M}, E) = \bigcup \mathfrak{H}(\mathfrak{O}, E)$. Dann ist f also in einem Raume $\mathfrak{H}(\mathfrak{O}, E)$ enthalten. Da die Topologie in $\mathfrak{H}(\mathfrak{M}, E)$ gröber ist als die von $\mathfrak{H}(\mathfrak{O}, E)$, kann f nach Satz 5 durch Funktionen aus $\mathfrak{H}(\mathfrak{O}, E_0)$ approximiert werden. Da $\mathfrak{H}(\mathfrak{O}, E_0)$ aber in $\mathfrak{H}(\mathfrak{M}, E_0)$ enthalten ist, gehören die approximierenden Funktionen also dem Raume $\mathfrak{H}(\mathfrak{M}, E_0)$ an.

§ 3. Der zu $\mathfrak{H}(\mathfrak{M}, E)$ duale Raum.

Wir wollen nun die Gesamtheit der stetigen linearen Funktionale auf $\mathfrak{H}(\mathfrak{M}, E)$, d. h. den zu $\mathfrak{H}(\mathfrak{M}, E)$ dualen Raum, bestimmen. Es bedeutet offenbar keine Einschränkung der Allgemeinheit, wenn wir annehmen, daß die Riemannsche Fläche $\mathfrak{R}$ offen ist. Denn ist $\mathfrak{M}$ eine echte Teilmenge von $\mathfrak{R}$, so gibt es stets eine offene Fläche $\mathfrak{R}' < \mathfrak{R}$, die $\mathfrak{M}$ umfaßt.

Ist aber $\mathfrak{R}$ eine kompakte Fläche und $\mathfrak{M} = \mathfrak{R}$, so besteht der Raum $\mathfrak{H}(\mathfrak{M}, E)$ nur aus den konstanten Funktionen, ist also zu E topologisch isomorph. Im folgenden sei also $\mathfrak{M}$ Teilmenge der offenen Fläche $\mathfrak{R}$. Ist $u[f(p)]$ ein stetiges lineares Funktional auf $\mathfrak{H}(\mathfrak{M}, E)$, so bildet u eine ganze Umgebung

$$\mathfrak{U}_2(\mathfrak{M}, \{\mathfrak{O}, \mathfrak{G}_\mathfrak{C}, V_\mathfrak{C}\}) = \Gamma\, \mathfrak{U}_1(\mathfrak{O}, \mathfrak{G}_\mathfrak{C}, V_\mathfrak{C}) \tag{15}$$

in den Einheitskreis ab. u ist also erst recht auf $\mathfrak{H}(\mathfrak{O}, E)$ für beliebiges $\mathfrak{O} \in \mathfrak{S}(\mathfrak{M})$ stetig.

Eine beliebige Funktion $f \in \mathfrak{H}(\mathfrak{M}, E)$ ist noch lokalanalytisch auf einer offenen Menge $\mathfrak{O} \in \mathfrak{S}(\mathfrak{M})$, gehört also zu $\mathfrak{H}(\mathfrak{O}, E)$. Da u die Umgebung

$$\mathfrak{U}_1(\mathfrak{O}, \mathfrak{G}_\mathfrak{C}, V_\mathfrak{C}) = \mathfrak{U}_0(\mathfrak{G}_\mathfrak{C}, V_\mathfrak{C}) \frown \mathfrak{H}(\mathfrak{O}, E)$$

[15]) *J. Sebastiao e Silva*, [8], S. 43—44.

in den Einheitskreis abbildet, ist u stetig in dem Raume $\mathfrak{B}(\mathfrak{G}_{\mathfrak{C}}, E)$. Da dieser Raum lokalkonvex ist, läßt sich das Funktional u stetig auf den ganzen Raum $\mathfrak{B}(\mathfrak{G}_{\mathfrak{C}}, E)$ fortsetzen zu einem Funktional $\bar{u}$, das $\mathfrak{U}_0(\mathfrak{G}_{\mathfrak{C}}, V_{\mathfrak{C}})$ in den Einheitskreis abbildet. (Es zeigt sich später, daß $\mathfrak{H}(\mathfrak{O}, E)$ in $\mathfrak{B}(\mathfrak{G}_{\mathfrak{C}}, E)$ dicht ist, so daß die Fortsetzung $\bar{u}$ durch u eindeutig bestimmt ist.) Ist nun $\bar{\mathfrak{H}}$ ein abgeschlossenes Teilgebiet von $\mathfrak{O}$, das $\mathfrak{G}_{\mathfrak{O}}$ ganz im Innern enthält und einen rektifizierbaren Rand besitzt, und ist $A(q, p)$ eine Elementarfunktion 1. Ordnung auf $\mathfrak{R}$, so gilt in $\mathfrak{H}$:

$$f(p) = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\bar{\mathfrak{H}}} f(q)\, A(q, p)\, dq. \tag{16}$$

Da die Riemannschen Summen des Integrals nach Satz 1 in $\mathfrak{G}_{\mathfrak{O}}$ gleichmäßig, also im Sinne der Topologie $\mathfrak{T}_0$ in $\mathfrak{B}(\mathfrak{G}_{\mathfrak{C}}, E)$ konvergieren, ist das Funktional $\bar{u}$ mit der Integration vertauschbar:

$$u[f] = u[f] = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\bar{\mathfrak{H}}} \bar{u}_p[f(q) \cdot A(q, p)]\, dq.$$

Wir untersuchen nun das Funktional $\bar{u}[x \cdot A(q, p)]$ für irgendein $q \in \mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{O}} = \mathfrak{R} - \overline{\mathfrak{G}}_{\mathfrak{C}}$. Da $A(q, p)$ für jedes q als Funktion von $p \in \overline{\mathfrak{G}}_{\mathfrak{C}}$ gleichmäßig beschränkt ist, hängt $\bar{u}[x \cdot A(q, p)]$ für jedes q stetig von x ab, ist also ein stetiges lineares Funktional auf E:

$$u[x \cdot A(q, p)] = u'(q)\,[x] = \langle x, u'(q)\rangle. \tag{17}$$

$u'(q)$ ist also eine in $\mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{C}}$ definierte Funktion mit Werten aus dem zu E dualen Raum E' und wir haben:

$$u[f] = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\bar{\mathfrak{H}}} \langle f(q), u'(q)\rangle\, dq. \tag{18}$$

Wir können nun zeigen, daß $u'(q)$ eine analytische Funktion mit Werten in E' ist.

Sei B eine beschränkte Menge in E und x ein Element aus B, ferner τ eine Ortsuniformisierende in $q_0 \in \mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{C}}$. Dann konvergiert $\frac{1}{h}\{A(q(\tau) + h), p) - A(q(\tau), p)\}$ für $h \to 0$ gegen $\frac{\partial}{\partial \tau} A(q(\tau), p)$ und zwar gleichmäßig in $p \in \mathfrak{G}_{\mathfrak{C}}$, da $A(q, p)$ analytisch ist. $\left\langle x, \frac{1}{h}\{u'(q(\tau + h)) - u'(q(\tau))\}\right\rangle = \bar{u}\left[x \cdot \frac{1}{h}\{A(q(\tau + h), p) - A(q(\tau), p)\}\right]$ konvergiert also gleichmäßig für alle $x \in B$ gegen $\bar{u}\left[x \cdot \frac{\partial}{\partial \tau} A(q(\tau), p)\right]$. Das heißt aber, $u'(q)$ ist eine analytische Funktion von q mit Werten in dem zu E dualen Raum E' mit der starken Topologie $\mathfrak{T}_b = \mathfrak{T}_b(E', E)$ für $q \in \mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{C}}$.

Da $\mathfrak{O}$ eine beliebige offene Menge aus $\mathfrak{S}(\mathfrak{M})$ war, gibt es also zu jedem $\mathfrak{O}^* \in \mathfrak{S}(\mathfrak{M})$ eine Menge $\mathfrak{G}_{\mathfrak{C}^*}$, derart, daß $u'(q)$ in $\mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{C}^*}$ analytisch ist. $u'(q)$ ist also auch analytisch in der Vereinigung

$$\mathfrak{U}' = \cup\, \mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{C}^*} = \mathbf{C} \cap \overline{\mathfrak{G}}_{\mathfrak{C}^*} > \mathbf{C}\mathfrak{M}.$$

$\mathfrak{U}'$ ist eine offene Menge, deren Komplement eine kompakte Teilmenge von $\mathfrak{M}$ ist. $u'(q)$ definiert also eine lokalanalytische Funktion in $\mathbf{C}\mathfrak{M}$, d. h. es ist $u'(q) \in \mathfrak{H}(\mathbf{C}\mathfrak{M}, E')$.

Darüber hinaus ist $u'(q)$ lokal gleichgradig stetig, d. h. zu jedem $q_0 \in \mathfrak{U}'$ gibt es eine Umgebung $\mathfrak{U}(q_0)$, derart, daß alle $u'(q)$, mit $q \in \mathfrak{U}(q_0)$ gleichgradig stetige lineare Abbildungen von E in den Körper der komplexen Zahlen sind.

$q_0 \in \mathfrak{U}'$ ist enthalten in einer der oben benutzten Mengen $\mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{C}^*}$. Man kann $\mathfrak{U}(q_0)$ also so wählen, daß es ganz im Innern von $\mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{C}^*}$ enthalten ist. Dann ist $A(q, p)$ für $q \in \mathfrak{U}(q_0)$, $p \in \overline{\mathfrak{G}}_{\mathfrak{C}^*}$ beschränkt durch eine Konstante M.

Da für $f \in \mathfrak{U}_0(\mathfrak{G}_{\mathfrak{C}^*}, V_{\mathfrak{C}^*})$ stets $|\bar{u}[f]| \leqq 1$ gilt, erhält man

$$|\langle x, u'(q)\rangle| = |u[x \cdot A(q, p)] \leqq \varepsilon \text{ für } q \in \mathfrak{U}(q_0)$$

und alle x aus der Umgebung $V = \frac{\varepsilon}{M} \cdot V_{\mathfrak{C}^*}$.

Wir haben also bewiesen:

Satz 8. *Jedem stetigen linearen Funktional $u[f]$ auf $\mathfrak{H}(\mathfrak{M}, E)$ läßt sich eine lokal gleichgradig stetige Funktion $u'(q)$ aus dem Raume $\mathfrak{H}(\mathbf{C}\mathfrak{M}, E')$ zuordnen, derart daß*

$$u[f] = \frac{1}{2\pi i} \int_{\mathrm{Rd}\,\bar{\mathfrak{H}}} \langle f(q), u'(q)\rangle\, dq$$

ist, wobei $\bar{\mathfrak{H}}$ ein abgeschlossenes Gebiet mit stückweise glattem Rand ist, derart, daß $f(q)$ in $\bar{\mathfrak{H}}$ und $u'(q)$ in $\mathbf{C}\mathfrak{H}$ analytisch ist. $u'(q)$ gestattet die Darstellung

$$(19) \quad \begin{cases} \langle x, u'(q)\rangle = \dfrac{1}{2\pi i} \displaystyle\int_{\mathrm{Rd}\,\bar{\mathfrak{H}}} \langle x \cdot A(q, p), u'(p)\rangle\, dp, \\[2ex] u'(q) = \dfrac{1}{2\pi i} \displaystyle\int_{\mathrm{Rd}\,\bar{\mathfrak{H}}} A(q, p)\, u'(p)\, dp \quad \text{für } q \in \mathbf{C}\mathfrak{H}. \end{cases}$$

$\mathfrak{H}^0(\mathbf{C}\mathfrak{M}, E')$ sei die Gesamtheit aller Funktionen mit Werten aus E', die im Komplement einer kompakten Teilmenge von $\mathfrak{M}$ analytisch und lokal gleichgradig stetig sind, wobei zwei Funktionen, die im Komplement einer kompakten Teilmenge von $\mathfrak{M}$ übereinstimmen, identifiziert werden.

Definition 6. *Eine Funktion $f(p)$ heiße in $\mathbf{C}\mathfrak{M}$ bianalytisch (bezüglich $A(p, q)$), wenn $f(p)$ im Komplement einer kompakten Teilmenge $\mathfrak{K}$ von $\mathfrak{M}$ analytisch ist und*

$$f(p) = \frac{1}{2\pi i} \int_{\mathrm{Rd}\,\bar{\mathfrak{H}}} A(p, q)\, f(q)\, dq \quad \text{für } p \in \mathbf{C}\mathfrak{K}$$

ist, wobei $\bar{\mathfrak{H}}$ eine $\mathfrak{K}$ ganz im Innern enthaltende abgeschlossene Menge ist, die p nicht enthält. Zwei Funktionen, die im Komplement einer kompakten Teilmenge von $\mathfrak{M}$ übereinstimmen, werden dabei als identisch angesehen.

Ist z. B. $\mathfrak{K}$ die offene Ebene und $A(\zeta, z) = (\zeta - z)^{-1}$, so ist eine Funktion $f(z)$ in einer Menge $\mathbf{C}\mathfrak{M} = \mathfrak{K} - \mathfrak{M}$ bianalytisch, wenn $f(z)$ in $\mathbf{C}\mathfrak{M}$ und ∞ analytisch ist und in ∞ verschwindet.

$f(z)$ ist also bianalytisch in $\mathbf{C}\mathfrak{M}$ dann und nur dann, wenn $f(z)$ in $\Omega - \mathfrak{M} = \mathbf{C}\mathfrak{M} \cup \infty$ im Sinne von L. Fantappié[16]) *biregulär* ist.

Es sei nun $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$ die Gesamtheit der in $\mathbf{C}\mathfrak{M}$ bianalytischen Funktionen mit Werten aus E', deren Werte lokal gleichgradig stetige lineare Funktionale auf E sind. Die den stetigen linearen Funktionalen $u[f]$ auf $\mathfrak{H}(\mathfrak{M}, E)$ zugeordneten Funktionen $u'(q)$ gehören also dem Raume $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$ an.

Sei nun $u'(q)$ ein beliebiges Element von $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$. Es ist im Komplement einer kompakten Teilmenge $\mathfrak{K} < \mathfrak{M}$ analytisch und lokal gleichgradig stetig.

---

[16]) Vgl. *P. Lévy*, Problèmes concrètes d'analyse fonctionelle, Quatrième Partie (par *F. Pellegrino*). Paris 1951.

Sei $\mathfrak{D} < \mathfrak{S}(\mathfrak{M})$ und $\overline{\mathfrak{G}}_{\mathfrak{D}}$ eine kompakte Teilmenge von $\mathfrak{D}$, die $\mathfrak{K}$ ganz im Innern enthält. $u'(q)$ ist auf der kompakten Menge $\mathrm{Rd}\,\overline{\mathfrak{G}}_{\mathfrak{D}}$ gleichgradig stetig, also gilt $|\langle x, u'(q)\rangle| \leqq 1$ für alle x aus einer Umgebung $V_{\mathfrak{D}} \in E$. Ist $\lambda_{\mathfrak{D}} = \dfrac{2\pi}{\int\limits_{\mathrm{Rd}\,\overline{\mathfrak{G}}_{\mathfrak{D}}} d\underline{p}}$, so bildet das durch

$$u[f] = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\overline{\mathfrak{G}}_{\mathfrak{D}}} \langle f(q), u'(q)\rangle\, d\underline{q} \tag{20}$$

definierte Funktional die Umgebung $\mathfrak{U}_1(\mathfrak{D}, \mathfrak{G}_{\mathfrak{D}}, \lambda_{\mathfrak{D}} V_{\mathfrak{D}}) < \mathfrak{H}(\mathfrak{D}, E)$ in den Einheitskreis ab, und $u[f]$ ist von der Wahl von $\overline{\mathfrak{G}}_{\mathfrak{D}}$ unabhängig, da $\langle f(q), u'(q)\rangle$ eine komplexwertige, analytische Funktion ist. $u[f]$ ist also ein stetiges lineares Funktional auf $\mathfrak{H}(\mathfrak{D}, E)$. Da dies für jedes $\mathfrak{D} \in \mathfrak{S}(\mathfrak{M})$ gilt, ist u auch stetig auf $\mathfrak{H}(\mathfrak{M}, E)$; denn es gilt $|u[f]| \leqq 1$ für alle

$$f \in \mathfrak{U}_2(\mathfrak{M}, \{\mathfrak{D}, \mathfrak{G}_{\mathfrak{D}}, \lambda_{\mathfrak{D}} V_{\mathfrak{D}}\}) = \Gamma\, \mathfrak{U}_1(\mathfrak{D}, \mathfrak{G}_{\mathfrak{D}}, \lambda_{\mathfrak{D}} V_{\mathfrak{D}}). \tag{21}$$

$u'(q)$ ist durch u eindeutig bestimmt:

$$\begin{aligned} \langle x, u'(q)\rangle &= \frac{1}{2\pi i} \int \langle x, A(q, p)\, u'(p)\rangle\, d\underline{p} \\ &= \frac{1}{2\pi i} \int \langle x \cdot A(q, p), u'(p)\rangle\, d\underline{p} = u_p[x \cdot A(q, p)]. \end{aligned} \tag{22}$$

Sei nun $\mathfrak{D} \in \mathfrak{S}(\mathfrak{M})$ und $\mathfrak{G}_{\mathfrak{D}} < \mathfrak{G}^*_{\mathfrak{D}} << \mathfrak{D}$ und $\mathfrak{G}^*_{\mathfrak{D}}$ relativ zu $\mathfrak{D}$ einfach zusammenhängend. Für $q \in \mathbf{C}\overline{\mathfrak{G}^*_{\mathfrak{D}}}$ läßt sich $x \cdot A(q, p)$ gleichmäßig auf $\overline{\mathfrak{G}^*_{\mathfrak{D}}}$ durch Funktionen

$$x \cdot f_{q,n}(p) \in \mathfrak{H}(\mathfrak{D}, E) < \mathfrak{H}(\mathfrak{M}, E)$$

approximieren[17]). Wegen (21) gilt dann aber

$$\bar{u}_p[x \cdot A(q, p)] = \lim_{n \to \infty} u[x \cdot f_{q,n}(p)]. \tag{23}$$

Damit ist $u'(q)$ in $\mathbf{C}\overline{\mathfrak{G}^*_{\mathfrak{D}}}$, und da $\mathfrak{D} \in \mathfrak{S}(\mathfrak{M})$ beliebig war, in $\cup\, \mathbf{C}\overline{\mathfrak{G}^*_{\mathfrak{D}}} = \mathbf{C} \cap \mathfrak{G}^*_{\mathfrak{D}} = \mathbf{C}\mathfrak{K}^* > \mathbf{C}\mathfrak{M}$ eindeutig durch die Werte des Funktionals u für Funktionen aus $\mathfrak{H}(\mathfrak{M}, E)$ bestimmt.

Die Abbildung $u \to u'(q)$ ist also eine Isomorphie des zu $\mathfrak{H}(\mathfrak{M}, E)$ dualen Raumes $\mathfrak{H}'(\mathfrak{M}, E)$ mit $\mathfrak{H}^0_{\Delta}(\mathbf{C}\mathfrak{M}, E')$.

Ist $w'(q)$ eine beliebige Funktion aus $\mathfrak{H}^0(\mathbf{C}\mathfrak{M}, E')$, so ist w' eindeutig zerlegbar in die Summe einer Funktion $v' \in \mathfrak{H}^0(\mathfrak{K}, E')$ und einer Funktion $u' \in \mathfrak{H}^0_{\Delta}(\mathbf{C}\mathfrak{M}, E')$:

$w'(q)$ ist analytisch im Komplement einer kompakten Teilmenge $\mathfrak{K} < \mathfrak{M}$.

$\overline{\mathfrak{H}}$ und $\overline{\mathfrak{G}}$ seien zwei kompakte Mengen, so daß $\mathfrak{K}$ ganz im Innern von $\overline{\mathfrak{H}}$ und $\overline{\mathfrak{H}}$ ganz im Innern von $\mathfrak{G}$ enthalten ist. In $\mathfrak{G} - \overline{\mathfrak{H}} = \mathfrak{G}_1$ gestattet $w'(q)$ die Darstellung

$$\begin{aligned} w'(q) &= \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\overline{\mathfrak{G}}_1} w'(p)\, A(p, q)\, d\underline{p} \\ &= \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\overline{\mathfrak{G}}} w'(p)\, A(p, q)\, d\underline{p} + \frac{-1}{2\pi i} \int\limits_{\mathrm{Rd}\,\overline{\mathfrak{H}}} w'(p)\, A(p, q)\, d\underline{p} \\ &= v'(q) \qquad\qquad + \quad u'(q). \end{aligned} \tag{24}$$

[17]) A. a. O. [1]).

$v'(q)$ ist analytisch und lokal gleichgradig stetig in $\mathfrak{G}$. Durch Änderung des Gebietes $\mathfrak{G}$ ändert sich aber $v'(q)$ nicht, und da $\mathfrak{G}$ beliebig groß gewählt werden kann, ist $v'(q)$ auf der ganzen Fläche $\mathfrak{R}$ analytisch und lokal gleichgradig stetig, gehört also zu $\mathfrak{H}^0(\mathfrak{R}, E')$.

$u'(q)$ ist im Komplement von $\overline{\mathfrak{H}}$ analytisch und lokal gleichgradig stetig. Da $\mathfrak{H}$ nur die kompakte Teilmenge $\mathfrak{K}$ im Innern enthalten muß, ist $u'(q)$ in $\mathbf{C}\mathfrak{K}$ analytisch und lokal gleichgradig stetig.

Für $v'(q)$ gilt jedenfalls

$$\int v'(p)\, A(p, q)\, dq = 0$$

und damit[18])

$$(25)\quad u'(q) = \frac{-1}{2\pi i} \int\limits_{\mathrm{Rd}\,\overline{\mathfrak{H}}} (w'(p) - v'(p))\, A(p, q)\, dp = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\overline{\mathfrak{H}}} u'(p)\, A(q, p)\, dp.$$

$u'(q)$ ist also bianalytisch in $\mathbf{C}\mathfrak{K}$, gehört also zu $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$. Eine Funktion $v' \in \mathfrak{H}^0(\mathfrak{R}, E')$, die bianalytisch in $\mathbf{C}\mathfrak{M}$ ist, verschwindet aber identisch. Denn es gilt dann

$$v'(q) = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\overline{\mathfrak{H}}} v'(p)\, A(q, p)\, dp.$$

Andererseits verschwindet aber das Integral, da der Integrand in $\mathfrak{H}$ analytisch ist. Die Zerlegung $w' = v' + u'$ ist also eindeutig, d. h. es gilt die direkte Summendarstellung

$$(25\text{a})\qquad \mathfrak{H}^0(\mathbf{C}\mathfrak{M}, E') = \mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E') \oplus \mathfrak{H}^0(\mathfrak{R}, E')$$

und damit

$$(26\text{b})\qquad \mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E') = \mathfrak{H}^0(\mathbf{C}\mathfrak{M}, E')/\mathfrak{H}^0(\mathfrak{R}, E').$$

Damit haben wir eine Darstellung des dualen Raumes zu $\mathfrak{H}(\mathfrak{M}, E)$ gefunden, die nicht mehr von der speziellen Wahl der Elementarfunktion abhängt.

Satz 9. *Der zu $\mathfrak{H}(\mathfrak{M}, E)$ duale Raum $\mathfrak{H}'(\mathfrak{M}, E)$ ist isomorph zu dem Raume $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$, der wieder zu dem Quotientenraum $\mathfrak{H}^0(\mathbf{C}\mathfrak{M}, E')/\mathfrak{H}^0(\mathfrak{R}, E')$ kanonisch isomorph ist. Die Isomorphie von $\mathfrak{H}'(\mathfrak{M}, E)$ und $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$ wird gegeben durch die Zuordnung*

$$(27)\qquad u \to u'(q), \quad \textit{wobei}\ \langle x, u'(q)\rangle = u_p[x \cdot A(q, p)]$$

ist. Die duale Paarung von $\mathfrak{H}(\mathfrak{M}, E)$ und $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, E')$ lautet

$$(28)\qquad u[f] = \langle f, u\rangle = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{H}} \langle f(p), u'(p)\rangle\, dp,$$

wobei $f(p)$ in $\overline{\mathfrak{H}}$ und $u'(p)$ in $\mathbf{C}\mathfrak{H}$ analytisch ist. Zwei Funktionen $u'_1(p)$ und $u'_2(p)$ aus $\mathfrak{H}^0(\mathbf{C}\mathfrak{M}, E')$ erzeugen dann und nur dann das gleiche Funktional u, wenn ihre Differenz auf der ganzen Fläche $\mathfrak{R}$ analytisch ist.

Korollar. *Ist $\mathfrak{M}_1$ relativ zu $\mathfrak{M}_2$ einfach zusammenhängend, so ist $\mathfrak{H}(\mathfrak{M}_2, E)$ in $\mathfrak{H}(\mathfrak{M}_1, E)$ dicht.*

Beweis. Jedes stetige lineare Funktional u auf $\mathfrak{H}(\mathfrak{M}_1, E)$ ist charakterisiert durch die in $\mathbf{C}\mathfrak{M}_1$ bianalytische Funktion

$$\langle x, u'(q)\rangle = u_p[x \cdot A(q, p)].$$

Wir wollen zeigen, daß $u'(q)$ durch die Werte von u für Funktionen aus $\mathfrak{H}(\mathfrak{M}_2, E)$ eindeutig bestimmt ist. Es gibt eine kompakte Teilmenge $\mathfrak{K} < \mathfrak{M}_1$, so daß $u'(q)$ in $\mathbf{C}\mathfrak{K}$ analytisch ist. Wir können annehmen, daß $\mathfrak{K}$ relativ zu $\mathfrak{M}_1$ einfach zusammenhängend ist.

[18]) Mit $A(p, q)$ ist nach Def. 4 auch $-A(q, p)$ eine Elementarfunktion 1. Ordnung auf $\mathfrak{R}$.

(Wäre das für $\mathfrak{K}$ noch nicht der Fall, so könnten wir $\mathfrak{K}$ zu einer relativ zu $\mathfrak{M}_1$ einfach zusammenhängenden kompakten Menge $\mathfrak{K}^* < \mathfrak{M}_1$ erweitern, indem wir zu $\mathfrak{K}$ alle Gebiete aus $\mathfrak{M}_1$, deren Rand in $\mathfrak{K}$ liegt, adjungieren.) Da $\mathfrak{K}$ relativ zu $\mathfrak{M}_1$ und $\mathfrak{M}_1$ relativ zu $\mathfrak{M}_2$ einfach zusammenhängend ist, ist $\mathfrak{K}$ offenbar relativ zu $\mathfrak{M}_2$ einfach zusammenhängend. Wir unterscheiden nun zwei Fälle:

a) $\mathfrak{M}_2$ ist kompakt. Dann enthält jede zusammenhängende Komponente von $\mathbf{C}\mathfrak{K}$ wenigstens einen Punkt von $\mathbf{C}\mathfrak{M}_2$. Nehmen wir nämlich an, $\mathfrak{G}$ sei eine Komponente, für die dies nicht richtig wäre, so ist $\mathfrak{G}$ ein Teilgebiet von $\mathfrak{M}_2$, dessen Rand zu $\mathfrak{K}$ gehört. Das ergibt also einen Widerspruch zu der Tatsache, daß $\mathfrak{K}$ relativ zu $\mathfrak{M}_2$ einfach zusammenhängend ist.

Zu jeder Komponente $\mathfrak{G}_i < \mathbf{C}\mathfrak{K}$ wählen wir einen Punkt $q_i \in \mathbf{C}\mathfrak{M}_2$ (t_i sei eine Ortsuniformisierende in q_i) aus. Die Funktion $u'(q)$ ist dann in $\mathbf{C}\mathfrak{K}$ vollständig bestimmt durch ihre Funktionselemente in den Punkten q_i, d. h. durch die Werte des Funktionals u für die zu $\mathfrak{H}(\mathfrak{M}_2, E)$ gehörigen Funktionen

$$\left\{\frac{\partial^\nu}{\partial t_i^\nu}\, x \cdot A(q(t_i), p)\right\}_{q=q_i} = \left\{x \cdot \frac{\partial^\nu}{\partial t_i^\nu}\, A(q(t_i), p)\right\}_{q=q_i} \qquad (\nu, i = 0, 1, 2, \ldots).$$

b) Ist $\mathfrak{M}_2$ nicht kompakt, so können wir für alle Komponenten $\mathfrak{G}_i < \mathbf{C}\mathfrak{K}$, die relativ kompakt in $\mathfrak{K}$ sind, die gleichen Schlüsse wie in a) durchführen. Für diejenige Komponente $\widetilde{\mathfrak{G}} < \mathbf{C}\mathfrak{K}$, deren Komplement kompakt ist (es gibt offenbar genau eine solche Komponente) kann es sein, daß $\widetilde{\mathfrak{G}}$ keinen Punkt von $\mathbf{C}\mathfrak{M}_2$ enthält. Daher wählen wir eine offene Menge $\mathfrak{G}^* \subsetneqq \mathfrak{K}$, die das Komplement von $\widetilde{\mathfrak{G}}$ ganz im Innern enthält und die relativ zu $\mathfrak{K}$ einfach zusammenhängend ist. Nach dem Approximationssatz von Behnke-Stein können wir die Funktion $A(q, p)$ für $q \in \mathbf{C}\mathfrak{G}^*$ gleichmäßig im Innern von $\mathfrak{G}^*$ durch Funktionen $f_{q,n}(p)$ approximieren, die auf der ganzen Fläche analytisch von p abhängen. Da die Konvergenz der $f_{q,n}$ also in einer ganzen Umgebung $\mathfrak{U}(\mathfrak{K})$ ($\mathfrak{K} < \mathfrak{U} < \overline{\mathfrak{U}} < \mathfrak{G}^*$) gleichmäßig ist, folgt:

$$\bar{u}_p[x \cdot A(q, p)] = \lim_{n \to \infty} \bar{u}_p[x \cdot f_{q,n}(p)] = \lim_{n \to \infty} u[x \cdot f_{q,n}(p)],$$

so daß also $u'(q)$ auch in $\widetilde{\mathfrak{G}}$ eindeutig durch die Werte von u für Funktionen aus $\mathfrak{H}(\mathfrak{M}_2, E)$ festgelegt ist. Wenn aber jedes stetige lineare Funktional in $\mathfrak{H}(\mathfrak{M}_1, E)$ bereits eindeutig durch seine Werte auf dem Teilraum $\mathfrak{H}(\mathfrak{M}_2, E)$ festgelegt ist, muß dieser Teilraum in $\mathfrak{H}(\mathfrak{M}_1, E)$ dicht sein, w. z. b. w.

Es ist

$$\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E') = \bigcup_{\mathfrak{K} < \mathfrak{M},\ \mathfrak{K} \text{ kompakt}} \mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, E'). \tag{29}$$

In $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, E')$ ist die Topologie $\mathfrak{T}_2$ definiert, da $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, E')$ in $\mathfrak{H}(\mathbf{C}\mathfrak{K}, E')$ enthalten ist. Die Topologie $\mathfrak{T}_2'$ in $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E') = \cup\, \mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, E')$ sei die Topologie der lokalkonvexen Hülle. Sie wird definiert durch die Umgebungen

$$\mathfrak{U}_2'(\mathbf{C}\mathfrak{M}, \{\mathbf{C}\mathfrak{K}, \mathfrak{G}_\mathfrak{K}, V_\mathfrak{K}'\}) = \Gamma_\mathfrak{K}\, \mathfrak{U}_0(\mathfrak{G}_\mathfrak{K}, V_\mathfrak{K}') \frown \mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, E'). \tag{30}$$

Falls $\overline{\mathfrak{M}}$ kompakt ist, stimmt in $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E')$ die Topologie $\mathfrak{T}_2'$ mit $\mathfrak{T}_2$ überein.

Wir suchen nun den zu $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E')$ dualen Raum zu bestimmen. Eine Funktion $u'(q) \in \mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E')$ ist in dem Komplement einer kompakten Teilmenge $\mathfrak{K} < \mathfrak{M}$ analytisch. Ein stetiges lineares Funktional $f[u'(q)]$ auf $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E')$ bildet eine Umgebung $\mathfrak{U}_2'(\mathbf{C}\mathfrak{M}, \{\mathbf{C}\mathfrak{K}, \mathfrak{G}_\mathfrak{K}, V_\mathfrak{K}'\})$, also auch $\mathfrak{U}_0(\mathfrak{G}_\mathfrak{K}, V_\mathfrak{K}') \frown \mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, E')$ in den Einheitskreis ab.

f ist also stetig in $\mathfrak{B}(\mathfrak{G}_\mathfrak{K}, V_\mathfrak{K}')$ und läßt sich stetig auf diesen ganzen Raum fortsetzen.

Ist nun $\mathfrak{H}_{\mathfrak{K}}$ eine kompakte Teilmenge, die $\mathfrak{K}$ ganz im Innern enthält und selbst ganz in $\mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{K}}$ enthalten ist, so gilt:

$$u'(q) = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{H}_{\mathfrak{K}}} A(q, p)\, u'(p)\, d\underline{p},$$

und da die Riemannschen Summen des Integrales auf $\overline{\mathfrak{G}}_{\mathfrak{K}}$ gleichmäßig konvergieren:

$$f[u'(q)] = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{H}_{\mathfrak{K}}} f_q[A(q, p)\, u'(p)]\, d\underline{p}. \tag{31}$$

$f_q[A(q, p) \cdot x']$ ist ein stetiges lineares Funktional auf E für jedes $p \in \mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{K}} > \mathfrak{K}$. Da $\mathfrak{K}$ eine beliebige kompakte Teilmenge von $\mathfrak{M}$ war, ist also für jedes p aus einer Umgebung von $\mathfrak{M}$ ein stetiges Funktional $\tilde{f}(p)$ auf E' definiert durch

$$\langle x', \tilde{f}(p)\rangle = f_q[A(q, p) \cdot x']. \tag{32}$$

Ist t eine Ortsuniformisierende in $p_0 \in \mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{K}}$, so konvergieren die Differenzenquotienten

$$\frac{1}{h}\{A(q, p(t+h)) - A(q, p(t))\}$$

in einer Umgebung $|t| \leqq \delta$ als Funktionen von q auf $\overline{\mathfrak{G}}_{\mathfrak{K}}$ gleichmäßig. Infolgedessen konvergieren die Differenzenquotienten von $A(q, p) \cdot x'$ für alle x' aus einer beliebigen beschränkten Menge im E' gleichmäßig für alle $p \in \mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{K}}$.

Berücksichtigt man wieder, daß $\mathfrak{K}$ eine beliebige kompakte Teilmenge von $\mathfrak{M}$ ist, so erhält man, daß $\tilde{f}(p)$ eine in $\mathfrak{M}$ analytische Funktion mit Werten in dem zu E' stark dualen Raume E'', $\tilde{f}(p) \in \mathfrak{H}(\mathfrak{M}, E'')$ ist.

Für das Funktional f erhält man die Darstellung

$$f[u'(q)] = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{H}_{\mathfrak{K}}} \langle u'(p), \tilde{f}(p)\rangle\, d\underline{p}. \tag{33}$$

Wir machen nun die Voraussetzung, daß E total reflexiv ist, d. h. es soll $E = E''$ sein und die starke Topologie in E'' mit der in E gegebenen Topologie $\mathfrak{T}_E$ übereinstimmen. Dann gehört also $\tilde{f}$ zu dem Raume $\mathfrak{H}(\mathfrak{M}, E)$.

Umgekehrt erzeugt auch jede Funktion $\tilde{f}(p) \in \mathfrak{H}(\mathfrak{M}, E)$ ein lineares Funktional f auf $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E')$. Wir zeigen, daß dieses Funktional stets stetig ist bezüglich der Topologie $\mathfrak{T}_2'$:

$\tilde{f}(p)$ ist analytisch in einer offenen Menge $\mathfrak{U} > \mathfrak{M}$. Sei $\mathfrak{K}$ eine beliebige kompakte Teilmenge von $\mathfrak{M}$ und $\mathfrak{K} << \mathfrak{H}_{\mathfrak{K}} << \mathfrak{U}$. Auf der kompakten Menge $\overline{\mathfrak{H}}_{\mathfrak{K}}$ ist $\tilde{f}(p)$ beschränkt. Es gibt also eine beschränkte kreiskonvexe Menge $B < E$ mit $\tilde{f}(p) \in B$ für alle $p \in \overline{\mathfrak{H}}_{\mathfrak{K}}$. Dann gilt für alle Funktionen $u'(p) \in \mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, E')$, die der Umgebung

$$\mathfrak{U}_2(\mathbf{C}\mathfrak{K}, \mathbf{C}\mathfrak{H}_{\mathfrak{K}} \cap \overline{\mathfrak{G}}_{\mathfrak{K}}, V_{\mathfrak{K}}') = \mathfrak{U}_0(\mathbf{C}\mathfrak{H}_{\mathfrak{K}} \cap \mathfrak{G}_{\mathfrak{K}}, V_{\mathfrak{K}}') \cap \mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, E')$$

mit $\mathfrak{G}_{\mathfrak{K}} >> \mathfrak{H}_{\mathfrak{K}}$ und $V_{\mathfrak{K}}' = \dfrac{2\pi}{\int\limits_{\mathrm{Rd}\,\mathfrak{H}_{\mathfrak{K}}} |d\underline{p}|} \cdot B^0$ angehören:

$$|\langle u'(p), \tilde{f}(p)\rangle| \leqq \frac{2\pi}{\int\limits_{\mathrm{Rd}\,\mathfrak{H}_{\mathfrak{K}}} |d\underline{p}|}, \text{ also } |f[u']| \leqq 1.$$

Die gleiche Abschätzung gilt dann für alle $u'(q)$ aus der konvexen Hülle

$$\mathfrak{U}_2'(\mathbf{C}\mathfrak{M}, \{\mathbf{C}\mathfrak{K}, \mathbf{C}\mathfrak{H}_{\mathfrak{K}} \cap \overline{\mathfrak{G}}_{\mathfrak{K}}, V_{\mathfrak{K}}'\}) = \Gamma\, \mathfrak{U}_2(\mathbf{C}\mathfrak{K}, \mathbf{C}\mathfrak{H}_{\mathfrak{K}} \cap \overline{\mathfrak{G}}_{\mathfrak{K}}, V_{\mathfrak{K}}').$$

Es ist also bewiesen:

Satz 10. *Der zu $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E')$ mit der Topologie $\mathfrak{T}_2'$ duale Raum ist isomorph zu $\mathfrak{H}(\mathfrak{M}, E)$, sofern nur E total-reflexiv ist.*

Nach dem Satz von Mackey-Arens[19]) ist die feinste Topologie in dem zu $\mathfrak{H}$ dualen Raum $\mathfrak{H}'$, die wieder $\mathfrak{H}$ als dualen Raum liefert, die Topologie $\mathfrak{T}_\tau$ der gleichmäßigen Konvergenz auf den schwach relativ kompakten Teilmengen von $\mathfrak{H}$. Nach Satz 10 ist also die Topologie $\mathfrak{T}_2'$ in $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E') \cong \mathfrak{H}'(\mathfrak{M}, E)$ gröber als die Topologie $\mathfrak{T}_\tau$ dieses Raumes.

In einem lokalkonvexen Vektorraum ist aber jede schwach relativ kompakte Menge schwach beschränkt uud jede schwach beschränkte Menge beschränkt. Das System der beschränkten Mengen in $\mathfrak{H}(\mathfrak{M}, E)$ enthält also alle schwach relativ kompakten Mengen. Damit ist die starke Topologie T_b in $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E')$ feiner als die Topologie T_τ. Es ist also auch $\mathfrak{T}_b$ feiner als die Topologie $\mathfrak{T}_2'$.

Korollar. *Ist E total reflexiv, so ist die starke Topologie $\mathfrak{T}_b$ in dem zu $\mathfrak{H}(\mathfrak{M}, E)$ dualen Raum $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, E')$ feiner als die Topologie $\mathfrak{T}_2'$.*

Für den Spezialfall, daß E der Körper der komplexen Zahlen ist, es sich also um komplexwertige analytische Funktionen handelt, können wir nun die Umkehrung beweisen.

Satz 11. *Die starke Topologie $\mathfrak{T}_b$ in dem zu $\mathfrak{H}(\mathfrak{M})$ dualen Raume $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M})$ stimmt mit der Topologie $\mathfrak{T}_2'$ überein. $\mathfrak{H}(\mathfrak{M})$ ist also reflexiv.*

Beweis. Sei $\mathfrak{B}$ eine beschränkte Menge in $\mathfrak{H}(\mathfrak{M})$. Es gibt dann eine offene Menge $\mathfrak{O} > \mathfrak{M}$ derart, daß $\mathfrak{B}$ in $\mathfrak{H}(\mathfrak{O})$ beschränkt ist (Satz 5). Ist $\mathfrak{K}$ eine beliebige kompakte Teilmenge von $\mathfrak{M}$, so gibt es eine kompakte Teilmenge $\widetilde{\mathfrak{K}} < \mathfrak{O}$, die $\mathfrak{K}$ ganz im Innern enthält. Auf $\widetilde{\mathfrak{K}}$ sind aber alle $f \in \mathfrak{B}$ gleichmäßig beschränkt:

$$|f(p)| \leqq B_{\widetilde{\mathfrak{K}}} \text{ für } p \in \widetilde{\mathfrak{K}} \text{ und } f \in \mathfrak{B}.$$

Die zu $\mathfrak{B}$ polare Menge $\mathfrak{B}^0$ aller Funktionale u', für die $|u[f]| \leqq 1$ ist für alle $f \in \mathfrak{B}$, enthält dann insbesondere die Umgebung $\mathfrak{U}_2(\mathbf{C}\mathfrak{K}, \overline{\mathfrak{G}}_{\widetilde{\mathfrak{K}}} \cap \mathbf{C}\widetilde{\mathfrak{K}}, V_{\widetilde{\mathfrak{K}}})$, wobei $\mathfrak{G}_{\widetilde{\mathfrak{K}}}$ die Menge $\widetilde{\mathfrak{K}}$ ganz im Innern enthält und $V_{\widetilde{\mathfrak{K}}} = \left\{x;\ |x| \cdot \int\limits_{\mathrm{Rd}\,\widetilde{\mathfrak{K}}} |dp| \frac{1}{2\pi} \cdot B_{\widetilde{\mathfrak{K}}} \leqq 1\right\}$ ist. Denn für $u'(q)$ aus dieser Umgebung gilt

$$\langle f(p), u'(p)\rangle \leqq 2\pi\left(\int |dp|\right)^{-1}.$$

Da die $\mathfrak{T}_b$-Umgebung $\mathfrak{B}^0$ konvex ist, enthält $\mathfrak{B}^0$ auch die konvexe Hülle

$$\mathfrak{U}_2'(\mathbf{C}\mathfrak{M}, \{\mathbf{C}\mathfrak{K}, \mathfrak{G}_{\widetilde{\mathfrak{K}}} \cap \mathbf{C}\widetilde{\mathfrak{K}}, V_{\widetilde{\mathfrak{K}}}\}) = \Gamma\, \mathfrak{U}_2(\mathbf{C}\mathfrak{K}, \mathfrak{G}_{\widetilde{\mathfrak{K}}} \cap \mathbf{C}\widetilde{\mathfrak{K}}, V_{\widetilde{\mathfrak{K}}}), \tag{34}$$

also eine $\mathfrak{T}_2'$-Umgebung in $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M})$. Die Topologie $\mathfrak{T}_2'$ ist also feiner als $\mathfrak{T}_b$. Da das Umgekehrte bereits gezeigt ist, folgt die Gleichheit beider Topologien.

Ist $E = E''$ und $\mathfrak{M} = \mathfrak{O}$ eine offene Menge auf $\mathfrak{R}$, so läßt sich der obige Beweis für die Übereinstimmung von $\mathfrak{T}_2'$ und $\mathfrak{T}_b$ in $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{O}, E')$ fast wörtlich übertragen, da in $\mathfrak{H}(\mathfrak{O}, E)$ auch jede beschränkte Menge auf jeder kompakten Teilmenge von $\mathfrak{O}$ gleichmäßig beschränkt ist. Es gilt also auch

Satz 12. *Ist E ein total-reflexiver Raum, so gilt für jede offene Menge $\mathfrak{O} < \mathfrak{R}$: In $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{O}, E')$ stimmt die starke Topologie $\mathfrak{T}_b$ mit der Topologie $\mathfrak{T}_2'$ überein.*

---

[19]) Vgl. *J. Dieudonné-L. Schwartz* [2], S. 64.

Es bleibt die Frage offen, ob dies auch für beliebige Mengen richtig ist. Es gilt jedenfalls, wenn man zeigen kann, daß jede beschränkte Menge in $\mathfrak{H}(\mathfrak{M}, E)$ in einem $\mathfrak{H}(\mathfrak{D}, E)$ mit $\mathfrak{D}$ aus $\mathfrak{S}(\mathfrak{M})$ enthalten und dort beschränkt ist[20]).

§ 4. Stetige lineare Abbildungen der Funktionenräume auf Riemannschen Flächen.

Für eine beliebige kompakte Teilmenge $\mathfrak{K} < \mathfrak{R}$ bestimmen wir die Gesamtheit der stetigen linearen Abbildungen des Raumes $\mathfrak{H}(\mathfrak{K}, E)$ in einen lokalkonvexen Vektorraum F.

Satz 13. *Ist $\mathfrak{K}$ eine kompakte Teilmenge der Riemannschen Fläche $\mathfrak{R}$ und F ein separierter lokalkonvexer Vektorraum, so gilt: Jeder stetigen linearen Abbildung T des Raumes $\mathfrak{H}(\mathfrak{K}, E)$ in den Raum F läßt sich eindeutig eine in $\mathbf{C}\mathfrak{K}$ bianalytische Funktion $\widetilde{T}(p)$ mit Werten aus dem Raum $\mathfrak{L}_b(E, F)$ der stetigen linearen Abbildungen von E in F zuordnen, wobei die $\widetilde{T}(p)$ lokal gleichgradig stetige Abbildungen von E in F sind, d. h. es gilt*

$$\widetilde{T} \in \mathfrak{H}^0_A(\mathbf{C}\mathfrak{K}, \mathfrak{L}_b(E, F)).$$

Umgekehrt erzeugt jede Funktion aus $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{K}, \mathfrak{L}_b(E, F))$ eine stetige Abbildung von $\mathfrak{H}(\mathfrak{K}, E)$ in den Raum F, sofern F halbvollständig (folgenvollständig) ist (oder falls in F die kreiskonvexe Hülle einer kompakten Menge stets wieder halbkompakt ist.) Dann gilt also:

$$\mathfrak{L}(\mathfrak{H}(\mathfrak{K}, E), F) \cong \mathfrak{H}^0_A(\mathbf{C}\mathfrak{K}, \mathfrak{L}_b(E, F)). \tag{35}$$

Die Isomorphie wird vermittelt durch die Zuordnung:

$$\begin{cases} \widetilde{T}(q)\,[x] =_{\mathrm{Df}} T[x \cdot A(q, p)]; \quad x \in E \\ T[f(p)] = \dfrac{1}{2\pi i} \displaystyle\int_{\mathrm{Rd}\,\mathfrak{U}(\mathfrak{K})} \widetilde{T}(p)\,[f(p)]\,dp\,. \end{cases} \tag{36}$$

Beweis. Ist $f(p) \in \mathfrak{H}(\mathfrak{K}, E)$, so läßt sich diese Funktion in einer offenen Menge $\mathfrak{U}(\mathfrak{K}) > \mathfrak{K}$ durch das Cauchyintegral $f(p) = \dfrac{1}{2\pi i} \displaystyle\int_{\mathrm{Rd}\,\mathfrak{U}(\mathfrak{K})} f(q)\,A(q, p)\,dq$ darstellen. Da die Riemannschen Summen des Integrals im Innern von $\mathfrak{U}(\mathfrak{K})$ gleichmäßig, also im Sinne der Topologie $\mathfrak{T}_2$ von $\mathfrak{H}(\mathfrak{K}, E)$ konvergieren, ist die Abbildung T mit dem Integral vertauschbar:

$$T[f(p)] = \frac{1}{2\pi i} \int T[f(q) \cdot A(q, p)]\,dq.$$

Für jedes $q \in \mathbf{C}\mathfrak{K}$ ist durch $\widetilde{T}(q)[x] = T_p[x \cdot A(q, p)]$ eine stetige lineare Abbildung von E in F definiert, da $A(q, p)$ als Funktion von p in einer Umgebung von $\mathfrak{K}$ beschränkt ist. Den Raum $\mathfrak{L}(E, F)$ der stetigen linearen Abbildungen versehen wir mit der Topologie $\mathfrak{T}_b$ der gleichmäßigen Konvergenz auf den beschränkten Teilmengen von E und bezeichnen den Raum dann mit $\mathfrak{L}_b(E, F)$. Wir zeigen nun, daß $\widetilde{T}(q)$ eine in $\mathbf{C}\mathfrak{K}$ analytische Funktion mit Werten aus $\mathfrak{L}_b(E, F)$ ist. Ist t eine Ortsuniformisierende in q, so ist

$$\frac{1}{h}\{A(q(t+h), p) - A(q(t), p)\} - \frac{\partial}{\partial t} A(q(t), p) \quad \text{für } h \to 0$$

auf einer Umgebung $\overline{\mathfrak{U}}_1(\mathfrak{K})$[21]) gleichmäßig konvergent gegen Null. Ist B eine beschränkte Menge aus E, so gibt es für jede Umgebung $V < E$ ein $\lambda = \lambda_V$, so daß $B < \lambda_V \cdot V$. Für alle h mit $|h| \leqq h_V$ gilt also

$$x \cdot \frac{1}{h}\{A(q(t+h), p) - A(q(t), p)\} - x \cdot \frac{\partial}{\partial t} A(q(t), p) \in V$$

für alle $x \in B$ und alle $p \in \overline{\mathfrak{U}}_1(\mathfrak{K})$.

[20]) Dann läßt sich der obige Beweis offenbar leicht übertragen.

[21]) $\mathfrak{U}_1(\mathfrak{K})$ ist so zu wählen, daß es zu einer Umgebung von q disjunkt und $f(p)$ auf $\overline{\mathfrak{U}}_1(\mathfrak{K})$ noch analytisch ist.

Zu jeder Umgebung $W < F$ gibt es nun wegen der Stetigkeit von T eine Umgebung $\tilde{\mathfrak{U}}_2(\mathfrak{K}, \{\mathfrak{O}_i, \mathfrak{G}_i, V_i\})$, die durch T in W abgebildet wird. Da $\mathfrak{U}_1(\mathfrak{K})$ eines der $\mathfrak{G}_i$ enthält, gilt also

$$\mathfrak{U}_0(\mathfrak{U}_1(\mathfrak{K}), V_{i_0}) < \tilde{\mathfrak{U}}_2(\mathfrak{K}, \{\mathfrak{O}_i, \mathfrak{G}_i, V_i\})$$

und damit

$$T\left[x \cdot \frac{1}{h}\{A(q(t+h), p) - A(q(t), p)\}\right] - T\left[x \cdot \frac{\partial}{\partial t} A(q(t), p)\right] \in W$$

für alle $x \in B$, sofern nur $|h| \leqq h_{V_{i_0}}$ ist $(\mathfrak{G}_{i_0} < \mathfrak{U}_1(\mathfrak{K}))$. Für $h \to 0$ konvergiert also $\dfrac{\tilde{T}(q(t+h)) - \tilde{T}(q(t))}{h}$ auf jeder beschränkten Teilmenge von E gleichmäßig im Sinne der Topologie $\mathfrak{T}_F$ von F. Die Funktion $\tilde{T}$ gehört also zu $\mathfrak{H}(\mathbf{C}\mathfrak{K}, \mathfrak{L}_b(E, F))$ und es gilt:

$$T[f(p)] = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{U}(\mathfrak{K})} \tilde{T}(q)[f(q)]\, dq = \frac{1}{2\pi i} \int \tilde{T}(p)[f(p)]\, dp, \tag{37}$$

wobei $\mathfrak{U}(\mathfrak{K})$ so gewählt ist, daß es $\mathfrak{K}$ ganz im Innern enthält und $f(p)$ in $\bar{\mathfrak{U}}(\mathfrak{K})$ noch analytisch ist.

Setzt man speziell $f(p) = x \cdot A(q, p)$, so erhält man:

$$T_p[x \cdot A(q, p)] = \tilde{T}(q)[x] = \frac{1}{2\pi i} \int \tilde{T}(p)[x \cdot A(q, p)]\, dp$$
$$= \frac{1}{2\pi i} \int A(q, p)\, \tilde{T}(p)[x]\, dp = \left(\frac{1}{2\pi i} \int A(q, p)\, \tilde{T}(p)\, dp\right)[x],$$

also

$$\tilde{T}(q) = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{U}(\mathfrak{K})} A(q, p)\, \tilde{T}(p)\, dp, \tag{38}$$

d. h. $\tilde{T}(q)$ ist bianalytisch in $\mathbf{C}\mathfrak{K}$.

Weiterhin ist aber $\tilde{T}(q)$ auch lokal gleichgradig stetig:

Ist $q_0 \in \mathfrak{U}_1(\mathfrak{K})$, so gibt es eine Umgebung $\bar{\mathfrak{U}}(q_0)$, die zu $\bar{\mathfrak{U}}_1(\mathfrak{K})$ disjunkt ist. $A(q, p)$ ist auf $\bar{\mathfrak{U}}(q_0)_q \times \bar{\mathfrak{U}}_1(\mathfrak{K})_p$ beschränkt durch eine Konstante M. Nun gibt es ja zu jeder Umgebung $W < F$ eine Umgebung $V < E$, so daß

$$T[\mathfrak{U}_0(\mathfrak{U}_1(\mathfrak{K}), V)] < W.$$

Dann gilt aber für alle $x \in V_1 = M^{-1} \cdot V$

$$\tilde{T}(q)[x] = T[x \cdot A(q, p)] < W \quad \text{für alle } q \in \bar{\mathfrak{U}}(q_0).$$

$\tilde{T}(q)$ ist also lokal gleichgradig stetig, gehört also dem Raume $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, \mathfrak{L}_b(E, F))$ an.

Sei nun umgekehrt $\tilde{T}(q) \in \mathfrak{H}_A^0(\mathbf{C}\mathfrak{K}, \mathfrak{L}_b(E, F))$. Ist $f(p) \in \mathfrak{H}(\mathfrak{K}, E)$, also $f(p)$ in einer Umgebung $\bar{\mathfrak{U}}(\mathfrak{K})$ noch analytisch, so ist $\tilde{T}(q)[f(q)]$ eine in $\mathbf{C}\mathfrak{K} \cap \mathfrak{U}(\mathfrak{K})$ analytische Funktion mit Werten aus F. Denn zunächst ist

$$\hat{T}_{A, p_\nu, x_\nu}(q) = \tilde{T}(q)[x_\nu \cdot A(p_\nu, q)] = A(p_\nu, q) \cdot \tilde{T}(q)[x_\nu]$$

für jedes $p_\nu \in \mathrm{Rd}\,\mathfrak{U}(\mathfrak{K})$, $x_\nu \in E$ eine für $q \in \mathbf{C}\mathfrak{K} \cap \mathfrak{U}(\mathfrak{K})$ analytische Funktion mit Werten in F. Also ist auch

$$\tilde{T}(q)\left[\frac{1}{2\pi i} \Sigma f(p_\nu) \cdot A(p_\nu, q)\, \Delta p_\nu\right] = \Sigma \frac{1}{2\pi i} \Delta p_\nu \hat{T}_{A, p_\nu, f(p_\nu)}(q) \in \mathfrak{H}(\mathbf{C}\mathfrak{K} \cap \mathfrak{U}(\mathfrak{K}), F).$$

Da nun $\frac{1}{2\pi i}\Sigma f(p_\nu)\cdot A(p_\nu, q)\,\Delta \underline{p}_\nu$ im Innern von $\mathfrak{C}\mathfrak{K} \cap \mathfrak{U}(\mathfrak{K})$ gleichmäßig im Sinne der Topologie $\mathfrak{T}_E$ gegen $f(q)$ konvergiert, ist wegen der gleichgradigen Stetigkeit der $\widetilde{T}(q)$ auch

$$\widetilde{T}(q)\,[f(q)] = \lim \Sigma \frac{1}{2\pi i}\,\Delta \underline{p}_\nu\,\hat{T}_{A,\,p_\nu,\,f(p_\nu)}(q) = \widetilde{T}(q)\left[\lim \frac{1}{2\pi i}\,\Sigma\, f(p_\nu)\,A(p_\nu, q)\,\Delta \underline{p}_\nu\right]$$

eine analytische Funktion in $\mathfrak{U}(\mathfrak{K}) \cap \mathfrak{C}\mathfrak{K}$ mit Werten in F. Daher existiert also für $\mathfrak{K} \ll \mathfrak{U}_1 \ll \mathfrak{U}(\mathfrak{K})$ das Integral $\frac{1}{2\pi i}\int\limits_{\mathrm{Rd}\,\mathfrak{U}_1} \widetilde{T}(q)\,[f(q)]\,d\underline{q}$ jedenfalls in der kompletten Hülle $\hat{F}$ von F. Da $\mathrm{Rd}\,\mathfrak{U}_1$ kompakt und $\widetilde{T}(q)\,[f(q)]$ als analytische Funktion auf $\mathrm{Rd}\,\mathfrak{U}_1$ gleichmäßig stetig ist, bilden die Funktionswerte $\widetilde{T}(q)\,[f(q)]$ für $q \in \mathrm{Rd}\,\mathfrak{U}_1$ eine kompakte Menge B in F. Ist $\Theta(B)$ die kreiskonvexe Hülle von B in F, so gehört das Integral $\frac{1}{2\pi i}\int\limits_{\mathrm{Rd}\,\mathfrak{U}_1} \widetilde{T}(q)[f(q)]d\underline{q}$ jedenfalls zu $\frac{1}{2\pi}\int |\,d\underline{q}\,|\,\overline{\Theta}(B)$, wobei $\overline{\Theta}(B)$ die abgeschlossene Hülle von $\Theta(B)$ in $\hat{F}$ ist. Ist nun die kreiskonvexe Hülle jeder kompakten Menge $B < F$ relativ halbkompakt in F[22]), so gehört auch $\frac{1}{2\pi i}\int \widetilde{T}(q)\,[f(q)]\,d\underline{q}$ zu F. Durch

$$T[f] = \frac{1}{2\pi i}\int\limits_{\mathrm{Rd}\,\mathfrak{U}_1} \widetilde{T}(q)\,[f(q)]\,d\underline{q}$$

wird dann eine lineare Abbildung von $\mathfrak{H}(\mathfrak{K}, E)$ in F definiert. Sei nun $\overline{\mathfrak{U}}_i$ eine beliebige abgeschlossene Umgebung von $\mathfrak{K}$. Da $\widetilde{T}(q)$ als lokal gleichgradig stetige Schar von Abbildungen von E in F auf der kompakten Menge $\mathrm{Rd}\,\overline{\mathfrak{U}}_i$ gleichgradig stetig ist, gibt es zu jeder Umgebung $W < F$ eine Umgebung $V_i \in E$, so daß $\widetilde{T}(q)\,[f(q)] \in \frac{2\pi}{\int\limits_{\mathrm{Rd}\,\mathfrak{U}_i} |\,d\underline{q}\,|}\cdot W$ für $f(q) \in V_i$ ist.

Dann gilt also auch für alle $f \in \mathfrak{U}_0(\mathfrak{U}_i, V_i)$

$$T[f] = \frac{1}{2\pi i}\int \widetilde{T}(q)\,[f(q)]\,d\underline{q} \in \overline{\Theta}(W)\,.$$

Ist nun F lokalkonvex, so gibt es ein fundamentales Umgebungssystem $\mathfrak{W} = \{W_\tau\}$ bestehend aus kreiskonvexen, abgeschlossenen Mengen, für die mithin $\overline{\Theta}(W_\tau) = W_\tau$ ist. Ist also $W < \mathfrak{W}$, so enthält W auch alle $T[f]$ für f aus der konvexen Hülle

$$\widetilde{\mathfrak{U}}_2(\mathfrak{K}, \{\mathfrak{U}_j, V_j\}) = \mathop{\Gamma}_{j=1}^{\infty} \mathfrak{U}_0(\mathfrak{U}_j, V_j)\,.$$

Zu jeder Umgebung W in F gibt es also eine Umgebung $\widetilde{\mathfrak{U}}_2$ in $\mathfrak{H}(\mathfrak{K}, E)$, die durch T in W abgebildet wird, d. h. T ist eine stetige Abbildung von $\mathfrak{H}(\mathfrak{K}, E)$ in F.

Ist also in F die kreiskonvexe Hülle jeder kompakten Menge relativ halbkompakt, so gilt die Isomorphie

$$(39)\quad \mathfrak{L}(\mathfrak{H}(\mathfrak{K}, E), F) \cong \mathfrak{H}^0_A(\mathfrak{C}\mathfrak{K}, \mathfrak{L}_b(E, F)) \cong \mathfrak{H}^0(\mathfrak{C}\mathfrak{K}, \mathfrak{L}_b(E, F))/\mathfrak{H}^0(\mathfrak{K}, \mathfrak{L}_b(E, F))\,.$$

Falls $\mathfrak{M}$ nicht kompakt ist, können nicht mehr alle stetigen linearen Abbildungen von $\mathfrak{H}(\mathfrak{M}, E)$ in den Raum F durch ein Integral der Form (36) dargestellt werden, wohl aber ist eine solche Darstellung für alle beschränkten Abbildungen von $\mathfrak{H}(\mathfrak{M}, E)$ in F möglich.

---

[22]) Diese Bedingung ist stets erfüllt, wenn der Raum F halbvollständig (folgenvollständig) ist.

Satz 14. *Jeder beschränkten linearen Abbildung T von $\mathfrak{H}(\mathfrak{M}, E)$ in den lokalkonvexen Vektorraum F läßt sich eindeutig eine in $\mathbf{C}\mathfrak{M}$ bianalytische Schar $\widetilde{T}(q)$ von lokal gleichgradig stetigen linearen Abbildungen von E in F zuordnen (d. h. $\widetilde{T} \in \mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$), so daß*

$$T[f] = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{U}_i} \widetilde{T}(q)\,[f(q)]\,dq$$

ist, wenn $f(q)$ in $\overline{\mathfrak{U}}_i$ und $\widetilde{T}(q)$ in $\mathbf{C}\mathfrak{U}_i$ analytisch ist.

Es ist $\widetilde{T}(q)[x] = T[x \cdot A(q, p)]$ für alle $x \in E$.

Umgekehrt erzeugt jede Funktion $\widetilde{T} \in \mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$ eine stetige lineare Abbildung $T[f] = \frac{1}{2\pi i} \int\limits_{\mathrm{Rd}\,\mathfrak{U}(\mathfrak{K})} \widetilde{T}(q)[f(q)]\,dq$ von $\mathfrak{H}(\mathfrak{M}, E)$ in F (durch die $\widetilde{T}(q)$ eindeutig bestimmt ist), sofern in F die kreiskonvexe Hülle jeder kompakten Menge relativ halbkompakt ist. T ist dann und nur dann beschränkt, wenn es eine beschränkte Menge $B < F$ gibt und die $\widetilde{T}(q)$ lokal gleichgradig beschränkt sind, so daß es zu jedem q_0 eine Umgebung $\overline{\mathfrak{U}}(q_0)$ gibt, derart, daß alle $\widetilde{T}(q)$ für $q \in \overline{\mathfrak{U}}(q_0)$ eine Umgebung $V_{\overline{\mathfrak{U}}(q_0)} < E$ in B abbilden.

Beweis. Ist $\widetilde{T} \in \mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$, so gibt es eine kompakte Teilmenge $\mathfrak{K}$ von $\mathfrak{M}$, so daß $\widetilde{T}$ auch zu $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{K}, \mathfrak{L}_b(E, F))$ gehört. Dann definiert $\widetilde{T}$ nach Satz 13 eine stetige lineare Abbildung von $\mathfrak{H}(\mathfrak{K}, E)$ in den Raum F (wenn in F die kreiskonvexe Hülle einer kompakten Menge stets relativ halbkompakt ist). Da $\mathfrak{H}(\mathfrak{M}, E)$ in $\mathfrak{H}(\mathfrak{K}, E)$ enthalten ist und die Topologie $\mathfrak{T}_2$ in $\mathfrak{H}(\mathfrak{M}, E)$ feiner ist als in $\mathfrak{H}(\mathfrak{K}, E)$, so ist die durch $\widetilde{T}(q)$ nach Satz 13 definierte Abbildung T von $\mathfrak{H}(\mathfrak{K}, E)$ in F auch in $\mathfrak{H}(\mathfrak{M}, E)$ stetig bezüglich der Topologie $\mathfrak{T}_2$.

Ist T eine beschränkte lineare Abbildung von $\mathfrak{H}(\mathfrak{M}, E)$ in F, so gibt es eine T_2-Umgebung $\mathfrak{U}_2(\mathfrak{M}, \{\mathfrak{O}, \mathfrak{G}_{\mathfrak{O}}, V_{\mathfrak{O}}\}$, die in eine beschränkte Menge $B < F$ abgebildet wird. Zu jeder Umgebung $W < F$ gibt es also ein $\lambda > 0$, so daß $\lambda B < W$ ist. Die Umgebung

$$\mathfrak{U}_1(\mathfrak{O}, \mathfrak{G}_{\mathfrak{O}}, \lambda V_{\mathfrak{O}}) = \mathfrak{U}_0(\mathfrak{G}_{\mathfrak{O}}, \lambda V_{\mathfrak{O}}) \cap \mathfrak{H}(\mathfrak{O}, E)$$

wird dann durch T in die Umgebung $W < F$ abgebildet. T ist also stetig in $\mathfrak{H}(\mathfrak{O}, E) \cap \mathfrak{B}(\mathfrak{G}_{\mathfrak{O}}, E)$ bezüglich der Topologie $\mathfrak{T}_0$ von $\mathfrak{B}(\mathfrak{G}_{\mathfrak{O}}, E)$. Nun ist aber $\mathfrak{H}(\mathfrak{O}, E)$ in $\mathfrak{H}(\overline{\mathfrak{G}}_{\mathfrak{O}}, E)$ dicht[23]), und die Topologie $\mathfrak{T}_2$ in $\mathfrak{H}(\overline{\mathfrak{G}}_{\mathfrak{O}}, E)$ ist feiner als die Topologie $\mathfrak{T}_0$ in $\mathfrak{B}(\mathfrak{G}_{\mathfrak{O}}, E)$. Also ist T in eindeutiger Weise fortsetzbar zu einer stetigen linearen Abbildung von $\mathfrak{H}(\overline{\mathfrak{G}}_{\mathfrak{O}}, E)$ in F, die wir auch wieder mit T bezeichnen können. T ist dann auf $\mathfrak{H}(\overline{\mathfrak{G}}_{\mathfrak{O}}, E) < \mathfrak{H}(\mathfrak{G}_{\mathfrak{O}}, E)$ eindeutig charakterisiert durch die in $\mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{O}} > \mathbf{C}\mathfrak{O}$ bianalytische Funktion $\widetilde{T}(q)$, die durch $\widetilde{T}(q)[x] = T[x \cdot A(p, q)]$ definiert ist.

$\widetilde{T}(q)$ ist dann offenbar auf die offene Menge $\cup\, \mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{O}} = \mathbf{C} \cap \overline{\mathfrak{G}}_{\mathfrak{O}} = \mathbf{C}\mathfrak{K} > \mathbf{C}\mathfrak{M}$ analytisch fortsetzbar und gehört dem Raume $\mathfrak{H}^0_A(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$ an. T ist aber auf jedem $\mathfrak{H}(\mathfrak{O}, E)$, also auch auf $\mathfrak{H}(\mathfrak{M}, E) = \cup\, \mathfrak{H}(\mathfrak{O}, E)$ durch $\widetilde{T}(q)$ eindeutig bestimmt. Die Zuordnung $T \leftrightarrow \widetilde{T}$ ist also eineindeutig. Wir wollen nun die den beschränkten Abbildungen T zugeordneten $\widetilde{T}(q)$ genau charakterisieren.

Sei nun $\mathfrak{A}$ eine kompakte Teilmenge aus den Komplement von $\overline{\mathfrak{G}}_{\mathfrak{O}}$. Dann ist $A(q, p)$ auf $\mathfrak{A}_q \times (\overline{\mathfrak{G}}_{\mathfrak{O}})_p$ beschränkt durch eine Konstante $M = M(\overline{\mathfrak{G}}_{\mathfrak{O}}, \mathfrak{A})$. Für $x \in M^{-1} \cdot V_{\mathfrak{O}} = V'_{\mathfrak{O}}$

[23]) Vgl. Korollar zu Satz 9.

gehört dann $x \cdot A(q, p)$ zu $\mathfrak{U}_0(\mathfrak{G}_\mathfrak{C}, V_\mathfrak{C})$, wird also durch T in die abgeschlossene Hülle $\bar{B}$ der beschränkten Menge $B < F$ abgebildet. Es gilt also für alle $q \in \mathfrak{A}$:

$$\tilde{T}(q)[x] = T[x \cdot A(q, p)] \in \bar{B} \quad \text{für alle } x \in V'_\mathfrak{C}.$$

Die $\tilde{T}(q)$ für $q \in \mathfrak{A}$ sind also gleichgradig beschränkte lineare Abbildungen von E in F mit der angegebenen Eigenschaft. Ist nun $\tilde{T}(q) \in \mathfrak{H}^0_A(\mathfrak{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$ und für eine beschränkte Menge $B < F$ lokal (d. h. für alle q aus einer Umgebung $\mathfrak{U}(q_0)$ eines beliebigen Punktes q_0 aus dem Definitionsgebiet von $\tilde{T}(q_0)$) $\tilde{T}(q)\, V_{q_0} < B$ für eine Umgebung $V_{q_0} < E$, so wählt man zu jedem $\mathfrak{O} < \mathfrak{S}(\mathfrak{M})$ eine kompakte Menge $\mathfrak{K}_\mathfrak{C} < \mathfrak{O}$, so daß der Rand von $\mathfrak{K}_\mathfrak{C}$ im Definitionsgebiet von $\tilde{T}$ liegt. $\tilde{T}(q)$ ist dann auf $\mathrm{Rd}\,(\mathfrak{K}_\mathfrak{C})$ gleichgradig beschränkt: Es gibt eine von q unabhängige Umgebung $V_\mathfrak{C} < E$, die durch $\tilde{T}(q)$ in die beschränkte Menge $B < F$ abgebildet wird für alle $q \in \mathrm{Rd}\,(\mathfrak{K}_\mathfrak{C})$.

Für $T[f] = \dfrac{1}{2\pi i} \displaystyle\int_{\mathrm{Rd}\,\mathfrak{K}_\mathfrak{C}} \tilde{T}(q)[f(q)]\, dq$ gilt also $T[f] \in \bar{B}$, falls[24])

$$f(q) \in \mathfrak{U}_0\left(\mathring{\mathfrak{K}}_\mathfrak{C}, \frac{2\pi}{\int_{\mathrm{Rd}\,\mathfrak{K}_\mathfrak{C}} |dq|} \cdot V_\mathfrak{C}\right) \cap \mathfrak{H}(\mathfrak{O}, E)$$

ist. Da B nicht von $\mathfrak{O}$ abhängt, gilt auch für alle f aus der konvexen Hülle

$$\mathfrak{U}_2\left(\mathfrak{M}, \{\mathfrak{O}, \mathring{\mathfrak{K}}_\mathfrak{C}, 2\pi \cdot \left(\int_{\mathrm{Rd}\,\mathfrak{K}_\mathfrak{C}} |dq|\right)^{-1} \cdot V_\mathfrak{C}\}\right)$$

die Relation $T[f] \in \bar{B}$, wenn man ohne Beschränkung der Allgemeinheit annimmt, daß $\bar{B}$ kreiskonvex ist. T ist also eine beschränkte Abbildung von $\mathfrak{H}(\mathfrak{M}, E)$ in den Raum F.

Damit ist Satz 14 vollständig bewiesen.

Es sei nun T eine beliebige stetige lineare Abbildung des Raumes $\mathfrak{H}(\mathfrak{M}, E)$ in den lokalkonvexen, separierten Vektorraum F. Zu jeder kreiskonvexen Umgebung $W < F$, d. h. zu jeder stetigen Halbnorm $N = N_W$, gibt es eine Umgebung $\mathfrak{U}_2(\mathfrak{M}, \{\mathfrak{O}, \mathfrak{G}_\mathfrak{C}, V_\mathfrak{C}\})$, die durch T in W abgebildet wird. Es ist also für alle f aus dieser Umgebung

$$N_W(T[f]) \leqq 1.$$

$\mathfrak{N}_N$ sei die Menge aller $y \in F$, für die $N(y) = 0$ ist, also ein linearer Teilraum von F. In dem Quotientenraum $F_N = F/\mathfrak{N}_N$ führen wir die Norm $\bar{N}(\bar{y}) = \bar{N}(y + \mathfrak{N}_N) =_{\mathrm{Df}} N(y)$ ein, die F_N zu einem normierten Raum macht.

φ_N sei die natürliche Abbildung von F auf F_N, die jedem y die Klasse $\bar{y} = y + \mathfrak{N}_N$ zuordnet, und $T_N[f] =_{\mathrm{Df}} \varphi_N \circ T[f]$. Dann ist T_N eine stetige lineare Abbildung von $\mathfrak{H}(\mathfrak{M}, E)$ in den normierten Raum F_N; denn für $f \in \mathfrak{U}_2(\mathfrak{M}, \{\mathfrak{O}, \mathfrak{G}_\mathfrak{C}, \lambda \cdot V_\mathfrak{C}\})$ gilt

$$\bar{N}(T_N[f]) \leqq \lambda.$$

$T_N[f]$ ist insbesondere auch in $\mathfrak{H}(\overline{\mathfrak{G}}_\mathfrak{C}, E)$ stetig, denn T_N bildet ein

$$\mathfrak{U}_2(\overline{\mathfrak{G}}_\mathfrak{C}, \{\mathfrak{O}^*, \mathfrak{G}_{\mathfrak{O}^*}, V_{\mathfrak{O}^*}\}_{\mathfrak{O}^* < \mathfrak{S}(\overline{\mathfrak{G}}_\mathfrak{O})}) < \mathfrak{U}_0(\mathfrak{G}_\mathfrak{C}, \lambda \cdot V_\mathfrak{C})\,^{25})$$

in die Umgebung $W_N(\lambda) = \{\bar{y};\, \bar{y} \in F_N \wedge \bar{N}(\bar{y}) \leqq \lambda\}$ ab. Da $\mathfrak{H}(\mathfrak{O}, E)$ in $\mathfrak{H}(\overline{\mathfrak{G}}_\mathfrak{C}, E)$ dicht liegt[26]), ist T_N in eindeutiger Weise zu einer stetigen linearen Abbildung von $\mathfrak{H}(\overline{\mathfrak{G}}_\mathfrak{O}, E)$ in F_N fortsetzbar.

---

[24]) $\mathring{\mathfrak{K}}$ sei das Innere von $\mathfrak{K}$, also $\mathring{\mathfrak{K}} = \mathfrak{C}\,(\mathfrak{C}\mathfrak{K})$.

[25]) Es genügt $\mathfrak{G}_{\mathfrak{C}^*} = \mathfrak{G}_\mathfrak{C}$ und $V_{\mathfrak{C}^*} = \lambda \cdot V_\mathfrak{C}$ zu wählen.

[26]) Vgl. a. a. O. [23]).

Nach Satz 13 ist T_N umkehrbar eindeutig eine Funktion $\widetilde{T}_N(q) \in \mathfrak{H}_A^0(\mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{D}}, \mathfrak{L}_b(E, F_N))$ zugeordnet.

$\widetilde{T}_N(q)$ ist dann aber auf $\bigcup_{\mathfrak{D} \in \mathfrak{S}(\mathfrak{M})} \mathbf{C}\overline{\mathfrak{G}}_{\mathfrak{D}} = \mathbf{C} \cap \overline{\mathfrak{G}}_{\mathfrak{D}} = \mathbf{C}\mathfrak{K} > \mathbf{C}\mathfrak{M}$ analytisch fortsetzbar, gehört also zu $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F_N))$. Wir haben der Abbildung $T \in \mathfrak{L}(\mathfrak{H}(\mathfrak{M}, E), F)$ also umkehrbar eindeutig ein System

$$(40) \qquad \widetilde{T}(q) = \{\widetilde{T}_N(q)\}, \quad \widetilde{T}_N(q) \in \mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F_N))$$

zugeordnet.

Ist N' eine Majorante von N, also $N'(y) \geqq N(y)$ für alle $y \in F$, so ist F_N Quotientenraum von $F_{N'}$. Ist $\varphi_{N',N}$ die natürliche Abbildung von $F_{N'}$ auf F_N, so gilt: $\varphi_N = \varphi_{N',N} \circ \varphi_{N'}$. Daher ist auch

$$T_N = \varphi_N \circ T = \varphi_{N',N} \circ \varphi_{N'} \circ T = \varphi_{N',N} \circ T_{N'}.$$

Dann gilt im Komplement einer kompakten Menge $\mathfrak{K} < \mathfrak{M}$:

$$\varphi_{N',N} \circ \widetilde{T}_{N'}(q) = \widetilde{T}_N(q).$$

Diese „Verträglichkeitsrelation" garantiert, daß es eine in $\mathbf{C}\mathfrak{M}$ definierte Funktion $\widetilde{T}(q)$[27]) gibt, so daß $\widetilde{T}_N(q) = \varphi_N \circ \widetilde{T}(q)$ ist. Nun sei umgekehrt $\widetilde{T}(q) = \{\widetilde{T}_N(q)\}$ mit $\widetilde{T}_N(q) \in \mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F_N))$ und $\widetilde{T}_N(q) = \varphi_{N',N} \circ \widetilde{T}_{N'}(q)$, wenn $N \leqq N'$ ist.

Nach Satz 14 definiert $\widetilde{T}_N(q)$ eine stetige lineare Abbildung

$$T_N[f] = \frac{1}{2\pi i} \int_{\mathrm{Rd}\,\mathfrak{H}_N} \widetilde{T}_N(q)[f(q)]\,dq = \frac{1}{2\pi i} \int_{\mathrm{Rd}\,\mathfrak{H}_N} (\varphi_{N',N} \circ \widetilde{T}_N(q))[f(q)]\,dq$$

von $\mathfrak{H}(\mathfrak{M}, E)$ in den Raum $\hat{F}_N$ und es gilt die Beziehung

$$T_N[f] = \varphi_{N',N}(T_{N'}[f]).$$

Wir setzen nun voraus, daß F vollständig ist. Aus einem Lemma von A. Grothendieck[28]) folgt dann, daß durch die $T_N[f] = \bar{y}_N$, die der Relation $\bar{y}_N = \varphi_{N',N}(\bar{y}_{N'})$ genügen, eindeutig ein Element $y = T[f] \in F$ definiert ist, so daß $T_N[f] = \varphi_N(T[f])$ für alle N gilt.

Dann ist also $T_N[f]$ nicht nur in $\hat{F}_N$, sondern in F_N enthalten. Man kann also die Mengen $\varphi_N^{-1}(T_N[f]) \in F$ bilden, die offenbar einen gegen $T[f]$ konvergenten Cauchyfilter erzeugen:

$$T[f] = \lim \{\varphi_N^{-1}(T_N[f])\}.$$

Die hierdurch definierte Abbildung von $\mathfrak{H}(\mathfrak{M}, E)$ in F ist stetig, denn für jede Umgebung $W = W_N < F$ gibt es eine Umgebung $\mathfrak{U}_2 < \mathfrak{H}(\mathfrak{M}, E)$, die durch T_N in W abgebildet wird. Da $\lambda \cdot \mathfrak{N}_N < W_N$ ist, gilt

$$T[f] \in W_N + \mathfrak{N}_N < W_N \quad \text{für alle } f \in \mathfrak{U}_2.$$

Der Formulierung der gewonnenen Resultate schicken wir eine Definition voraus:

Definition 7. *Unter einer in* $\mathbf{C}\mathfrak{M}$ *lokalanalytischen Funktion im weiteren Sinne mit stetigen linearen Abbildungen von E in F als Werten verstehen wir ein System* $\widetilde{T}(q) = \{\widetilde{T}_N(q)\}$,

---

[27]) $\widetilde{T}(q)$ ist eine im Innern von $\mathbf{C}\mathfrak{M}$ analytische Funktion mit Werten in $\mathfrak{L}_b(E, F)$.

[28]) A. a. O. [3]), § 6, 2. Lemma 1.

wobei $\widetilde{T}_N(q)$ eine in $\mathbf{C}\mathfrak{M}$ lokalanalytische Funktion mit Werten in $\mathfrak{L}_b(E, F_N)$ ist, und die ***Verträglichkeitsrelation***

$$\varphi_{N',N} \circ \widetilde{T}_{N'}(q) = \widetilde{T}_N(q)$$

erfüllt ist.

$\widetilde{T}(q)$ heiße ***lokalbianalytisch****, wenn jedes $\widetilde{T}_N(q)$ bianalytisch ist; es heiße* ***lokal gleichgradig stetig****, wenn jedes $\widetilde{T}_N(q)$ lokal (bezüglich q) gleichgradig stetige lineare Abbildungen von E in F_N darstellt.*

$\widetilde{\mathfrak{H}}^0_A(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$ sei der lineare Raum der in $\mathbf{C}\mathfrak{M}$ lokalbianalytischen Funktionen im weiteren Sinne, mit stetigen linearen Abbildungen von E in F, die lokal gleichgradig stetig sind, als Werten. Wir haben dann bewiesen:

Satz 15. *Jeder stetigen linearen Abbildung T des Raumes $\mathfrak{H}(\mathfrak{M}, E)$ in einen lokalkonvexen Vektorraum F entspricht umkehrbar eindeutig eine in $\mathbf{C}\mathfrak{M}$ lokalanalytische Funktion $\widetilde{T}(q) = \{\widetilde{T}_N(q)\}$ im weiteren Sinne aus $\widetilde{\mathfrak{H}}^0_A(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$.*

Ist F vollständig, so erzeugt auch jede Funktion $\widetilde{T}(q) = \{\widetilde{T}_N(q)\}$ aus $\widetilde{\mathfrak{H}}^0_A(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$ eine stetige lineare Abbildung T von $\mathfrak{H}(\mathfrak{M}, E)$ in F.

Die Zuordnung zwischen T und $\widetilde{T}$ ist gegeben durch:

$$\widetilde{T}_N(q)\,[x] =_{\mathrm{Df}} \varphi_N \circ T[x \cdot A(q, p)]$$

und

$$T[f] = \lim \varphi_N^{-1}(T_N[f] = \lim_N \varphi_N^{-1}\left(\frac{1}{2\pi i} \int_{\mathrm{Rd}\,\mathfrak{H}_N} \widetilde{T}_N(q)\,[f(q)]\,dq\right),$$

wobei $f(q)$ in $\bar{\mathfrak{H}}_N$, $\widetilde{T}_N(q)$ in $\mathbf{C}\mathfrak{H}_N$ analytisch ist.

Bei vollständigem F gilt also die Isomorphie

$$\mathfrak{L}(\mathfrak{H}(\mathfrak{M}, E), F) \cong \widetilde{\mathfrak{H}}^0_A(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F)).$$

Von besonderer Bedeutung ist natürlich der Fall, daß E der komplexe Zahlkörper K ist. Dann ist $\mathfrak{L}_b(K, F)$ zu F topologisch isomorph, denn eine stetige lineare Abbildung $\widetilde{T}$ von K in F ist durch das Element $y_{\widetilde{T}} = \widetilde{T}[1] \in F$ eindeutig bestimmt. Man überzeugt sich ohne Mühe, daß bei dieser Isomorphie $\widetilde{T} \leftrightarrow \widetilde{T}(1)$ von $\mathfrak{L}_b(K, F)$ und F die Topologie $\mathfrak{T}_b$ von $\mathfrak{L}_b(K, F)$ in die Topologie $\mathfrak{T}_F$ von F übergeht.

Eine lokalanalytische Funktion i. w. S. mit stetigen linearen Abbildungen von K in F als Werten kann also als lokalanalytische Funktion mit Werten in F aufgefaßt werden. Satz 15 läßt sich für $K = E$ also vereinfachen zu:

Korollar. *Jeder stetigen linearen Abbildung T von $\mathfrak{H}(\mathfrak{M})$ in F läßt sich eine in $\mathbf{C}\mathfrak{M}$ bianalytische Funktion $\widetilde{T}(q)$ i. w. S. mit Werten aus F zuordnen.*

Ist F vollständig, so erzeugt auch jede in $\mathbf{C}\mathfrak{M}$ bianalytische Funktion i. w. S. mit Werten aus F eine stetige lineare Abbildung

$$T[f] = \lim \varphi_N^{-1}\left(\frac{1}{2\pi i} \int_{\mathrm{Rd}\,\mathfrak{H}_N} \widetilde{T}_N(q) \cdot f(q)\,dq\right),$$

und $\widetilde{T}$ ist durch T eindeutig bestimmt.

Es gilt also die Isomorphie

$$\mathfrak{L}(\mathfrak{H}(\mathfrak{M}), F) \cong \widetilde{\mathfrak{H}}_A^0(\mathbf{C}\mathfrak{M}, F) = \widetilde{\mathfrak{H}}_A(\mathbf{C}\mathfrak{M}, F).$$

Zu beweisen ist nur noch, daß die gleichgradige Stetigkeit in diesem Fall trivial ist.

Sei also $\widetilde{T}_N(q)$ eine stetige Abbildung von K in F_N und $\widetilde{T}_N(q)$ analytisch bezüglich der Topologie $\mathfrak{T}_b$ in $\mathfrak{L}_b(K, F) \cong F$. Dann ist $\widetilde{T}(q)$ also erst recht stetig bezüglich $\mathfrak{T}_b$, d. h. zu jeder Umgebung W in F (und jeder beschränkten Menge $B_\lambda = \{x; |x| \leqq \lambda\}$) gibt es eine Umgebung $\mathfrak{U}(q)$, so daß für $q' \in \mathfrak{U}(q)$

$$\widetilde{T}_N(q)[x] - \widetilde{T}_N(q')[x] \in W \quad \text{für} \quad |x| \leqq \lambda$$

gilt. Da $\widetilde{T}_N(q)$ für festes q aber K stetig in F_N abbildet, gilt $\widetilde{T}_N(q)[x] \in W$ für $x \in V = B_\mu$, also $\widetilde{T}_N(q)'[x] \in 2W$ für alle $q' \in \mathfrak{U}(q)$ und alle $x \in B_{\min(\mu, \lambda)}$. Es ist also $\widetilde{T}_N(q) = \varphi_N \circ T[A(q, p)]$ eine Schar lokal gleichgradig stetiger Abbildungen. Also entspricht jeder in $\mathbf{C}\mathfrak{M}$ bianalytischen Funktion i. w. S. $\widetilde{T}(q)$ mit Werten aus F eine Funktion aus $\widetilde{\mathfrak{H}}_A^0(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(K, F))$.

Eine weitere Möglichkeit der Vereinfachung liegt vor, wenn F ein Banachraum ist. Dann ist jede analytische Funktion i. w. S. eine gewöhnliche analytische Funktion und es gilt:

Satz 16. *Ist F ein Banachscher Raum, so ist der Raum $\mathfrak{L}(\mathfrak{H}(\mathfrak{M}, E), F)$ isomorph zu $\mathfrak{H}_A^0(\mathbf{C}\mathfrak{M}, \mathfrak{L}_b(E, F))$ und $\mathfrak{L}(\mathfrak{H}(\mathfrak{M}), F) \cong \mathfrak{H}_A(\mathbf{C}\mathfrak{M}, F)$. Denn jede Funktion aus $\mathfrak{H}_A(\mathbf{C}\mathfrak{M}, F)$ definiert eine lokalgleichgradig stetige Schar von Abbildungen von K in F.*

Literaturverzeichnis.

[1] *H. Behnke-K. Stein*, Entwicklungen analytischer Funktionen auf Riemannschen Flächen. Math. Ann. **120**, 430—461 (1949.)

[2] *J. Dieudonné-L. Schwartz*, La dualité dans les espaces F et LF. Ann. Inst. Fourier **1**, 61—101 (1949).

[3] *A. Grothendieck*, Sur certaines espaces de fonctions holomorphes. I. J. reine angew. Math. **192**, 35—64 (1953).

[4] *G. Köthe*, Dualität in der Funktionentheorie. J. reine und angew. Math. **191**, 30—49 (1953).

[5] *G. Köthe*, Die Randverteilungen analytischer Funktionen, Math. Zeitschr. **58**, 13—33 (1953).

[6] *F. Pellegrino*, La théorie des fonctionelles analytiques et ses applications, in: *P. Lévy*, Problèmes concrètes d'analyse fonctionelles, Paris 1951.

[7] *J. Sebastiao e Silva*, As funcoes analyticas e a analise funcional. Thèse, Lissabon (1948). Veröffentlicht in Port. Math. **9** (1950).

[8] *J. Sebastiao e Silva*, Sui fundamenti della teoria dei funzionali analitici. Port. Math. **12**, 1—46 (1953).

[9] *H. G. Tillmann*, Randverteilungen analytischer Funktionen und Distributionen, Math. Zeitschr. **59**, 61—83 (1953).

[10] *H. G. Tillmann*, Dualität in der Potentialtheorie. Portugaliae Mathematica **13**, 55—86 (1954).

Eingegangen 25. Februar 1954.

A note on continued fractions and dimension theory.

By *Arwel Evans*, Cambridge.

1. Introduction.

An interesting problem of continued fractions and Hausdorff dimension is that of determining the dimension of the set formed when a_i in the continued fraction

$$\frac{1}{a_1+}\cdot\frac{1}{a_2+}\cdots\frac{1}{a_i+}\cdots$$

are restricted to take only given integer values.

An important result in dealing with this problem is given by Good [1] (p. 205) in theorem 11 of his paper, to which reference should be made for a bibliography of the subject. This result is :

Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be k different positive integers. Let E' be the set of continued fractions each of whose partial quotients is either $\alpha_1, \alpha_2, \ldots \alpha_{k-1}$ or α_k. Let $K(a_1, a_2, \ldots a_n)$ be the denominator of

$$\frac{1}{a_1+}\cdot\frac{1}{a_2+}\cdots\frac{1}{a_n}$$

when expanded. Then the equation

$$\sum_{\substack{a_1, a_2, \ldots, a_n \\ \text{(all possible combinations of } \alpha_1, \ldots, \alpha_k)}} K(a_1, a_2, \ldots a_n)^{-2t} = 1 \tag{1.1}$$

has an unique root τ_n, and τ_n tends to a limit τ as $n \to \infty$. Moreover dim $E' = \tau$.

We shall call this result theorem G, and we note that in the summation there are k^n different terms. The effect of theorem G is to transfer the problem to that of finding the distribution of the magnitudes of the $K(a_1, \ldots a_n)$ when the a_i are restricted to given integers.

Here we shall consider the case when we have only two integer values denoted by r and s. We shall obtain inequalities for the magnitude of $K(a_1, \ldots a_n)$ which lead to inequalities on the dimension of the set by theorem G.

To be precise we shall use the notation $Q(u, v)$ for $K(a_1, \ldots a_n)$ if $a_i = r$, u times and $a_i = s$, v times so that $u + v = n$. Then if

$$\varrho = r + \frac{1}{r+}\cdot\frac{1}{r+}\cdots, \qquad \sigma = s + \frac{1}{s+}\cdot\frac{1}{s+}\cdots \tag{1.2}$$

we shall show that

$$A_1 r^u s^v \leqq Q(u, v) \leqq A_2 \varrho^u \sigma^v \tag{1.3}$$

where A_1 and A_2 are positive constants independent of u and v. This will give, from theorem G, that the set $E(r, s)$, composed of continued fraction with quotients taking only the values r and s, has dimension $d = \dim E(r, s)$ satisfying

$$1 \geqq \varrho^{-2d} + \sigma^{-2d}, \tag{1.4}$$

$$1 \leqq r^{-2d} + s^{-2d}. \tag{1.5}$$

2. Formation of $Q(u, v)$.

$Q(u, v)$ is usually written as q_n and is a linear combination of q_{n-1} and q_{n-2} (see Good [1], p. 201), but in this case q_{n-1} must be a $Q(u-1, v)$ or $Q(u, v-1)$ and q_{n-2} must be a $Q(u-2, v)$, $Q(u-1, v-1)$ or $Q(u, v-2)$. In fact the form of the whole set of $Q(u, v)$ is that of a Pascal triangle, and we may represent the formation of $Q(u, v)$ diagramatically as follows:

$$\begin{array}{ccccc} Q(u, v-2) & & Q(u-1, v-1) & & Q(u-2, v) \\ & \diagdown & & \diagdown\diagup & \\ & Q(u, v-1) & & Q(u-1, v) & \\ & & \diagdown\diagup & & \\ & & Q(u, v) & & \end{array} \tag{2.1}$$

We see that each $Q(u, v)$ must be formed in one of four ways.

$$\text{(A)} \quad \begin{cases} \text{(i)} & Q(u, v) = r \cdot Q(u-1, v) + Q(u-2, v) \\ \text{(ii)} & Q(u, v) = r \cdot Q(u-1, v) + Q(u-1, v-1) \\ \text{(iii)} & Q(u, v) = s \cdot Q(u, v-1) + Q(u-1, v-1) \\ \text{(iv)} & Q(u, v) = s \cdot Q(u, v-1) + Q(u, v-2)\ . \end{cases}$$

For a_n and a_{n-1} are either r or s. (Note that the equation (i) only implies that $Q(u, v)$ is formed from *some* $Q(u-1, v)$, $Q(u-2, v)$.)

Equations (A) easily give the following result.

Theorem 1. $Q(u, v) \geqq A \cdot r^u \cdot s^v$.

This comes easily by induction on assuming the result true for $u + v \leqq n - 1$, and it is obviously true for $n = 1$. This gives the first half of (1. 3). We now prove the other half of (1. 3).

Theorem 2. $Q(u, v) \leqq A \cdot \varrho^u \cdot \sigma^v$.

3. The proof of theorem 2.

We first note that since $r \neq s$, we may suppose $s \geqq r + 1$. We also note that ϱ and σ satisfy the following equations:

$$\varrho^2 = r\varrho + 1 \text{ or } \varrho(\varrho - r) = 1, \tag{3.1}$$

$$\sigma^2 = s\sigma + 1 \text{ or } \sigma(\sigma - s) = 1. \tag{3.2}$$

We also need the following

Lemma 1. *If* $\varrho^2 = r\varrho + 1$, $\sigma^2 = s\sigma + 1$, *then*

$$r\varrho + s\sigma - s\varrho - r\sigma = (\sigma - \varrho)^2 + \varrho\sigma\left(\frac{1}{\varrho} - \frac{1}{\sigma}\right)^2.$$

Proof. Obviously we have from (3. 1) and (3. 2)

$$s\varrho + r\sigma - 2\varrho\sigma = \varrho\sigma\left(\frac{s}{\sigma} + \frac{r}{\varrho} - 2\right) = \varrho\sigma\left(-\frac{1}{\sigma^2} - \frac{1}{\varrho^2}\right)$$

and

$$\varrho^2 + \sigma^2 = r\varrho + s\sigma + 2.$$

Adding gives

$$s\varrho + r\sigma + (\sigma - \varrho)^2 = r\varrho + s\sigma - \varrho\sigma\left(\frac{1}{\varrho} - \frac{1}{\sigma}\right)^2.$$

We shall now prove theorem 2 by induction; as the contention is true for $n = 1$, we suppose that

$$(3.3) \qquad Q(u, v) \leqq A \cdot \varrho^u \cdot \sigma^v \text{ for } u + v \leqq n - 1.$$

We consider the cases (i) to (iv) in (A) separately. (i), (ii) and (iv) are straightforward.

In (i),

$$Q(u, v) \leqq r \cdot A \cdot \varrho^{u-1} \cdot \sigma^v + A\varrho^{u-2} \cdot \sigma^v$$
$$= A\,\varrho^u\sigma^v\left(\frac{r}{\varrho} + \frac{1}{\varrho^2}\right) = A\varrho^u\sigma^v$$

by (3.1). In (ii)

$$Q(u, v) \leqq r \cdot A\varrho^{u-1} \cdot \sigma^v + A \cdot \varrho^{u-1} \cdot \sigma^{v-1}$$
$$= A\varrho^u\sigma^v\left(\frac{r}{\varrho} + \frac{1}{\varrho\sigma}\right)$$
$$< A\varrho^u\sigma^v\left(\frac{r}{\varrho} + \frac{1}{\varrho^2}\right) = A\varrho^u\sigma^v$$

by (3.1) and since $\sigma > \varrho$. In (iv)

$$Q(u, v) \leqq s \cdot A\varrho^u\sigma^{v-1} + A\varrho^u\sigma^{v-2}$$
$$= A\varrho^u\sigma^v\left(\frac{s}{\sigma} + \frac{1}{\sigma^2}\right) = A\varrho^u\sigma^v$$

by (3.2).

We have to deal now with case (iii). We first note that $Q(u, 0) = K(r, r, \ldots, r)$ satisfies

$$(3.4) \qquad Q(u, 0) = \frac{\varrho^2}{\varrho^2 + 1} \cdot \varrho^u + \frac{1}{\varrho^2 + 1} \cdot (-\varrho)^{-u}.$$

This comes from direct calculation, since $Q(u, 0)$ satisfies

$$Q(u, 0) = r \cdot Q(u - 1, 0) + Q(u - 2, 0).$$

Now unless $v = 1$ in $Q(u, v) = K(a_1, \ldots, a_j, \ldots, a_n)$, (in which case the result follows from (3.4) on substituting in (A) (iii)), we must have $a_j = s$ for some $j \neq n$. Let the greatest such j be the number $j = n - i - 1$; then in $K(a_1, \ldots, a_n)$ we have $a_n = s$, and this is preceeded by a "block" of i r's, where $u \geqq i \geqq 1$. This means that $K(a_1, \ldots, a_j)$ is a $Q(u - i, v - 1)$, and $K(a_1, \ldots, a_{j-1})$ is a $Q(u - i, v - 2)$. So applying the induction hypothesis and (A) (ii) to $K(a_1, \ldots, a_{j-1})$ which is a $Q(u - i + 1, v - 1)$, and using the $Q(u, v)$ notation for convenience (although we are dealing with a special sequence, one with a block of i r's), we have

$$(3.5) \qquad Q(u - i + 1, v - 1) \leqq A\varrho^{u-i+1} \cdot \sigma^{v-1}\left(\frac{r}{\varrho} + \frac{1}{\varrho\sigma}\right)$$

giving from (A) (i)

$$(3.6) \qquad Q(u - i + 2, v - 1) \leqq A\varrho^{u-i+2} \cdot \sigma^{v-1}\left\{\frac{r}{\varrho}\left(\frac{r}{\varrho} + \frac{1}{\varrho\sigma}\right) + \frac{1}{\varrho^2}\right\}$$

provided $i > 1$.

When $i = 1$, we use (3. 5) and (A) (iii) to get

$$Q(u, v) \leqq A\varrho^u \cdot \sigma^v \left\{\frac{s}{\sigma}\left(\frac{r}{\varrho} + \frac{1}{\varrho\sigma}\right) + \frac{1}{\varrho\sigma}\right\}.$$

We have to show that the expression in brackets is $\leqq 1$, but

$$\begin{aligned}
\varrho\sigma^2 - rs\sigma - s - \sigma &= \varrho s\sigma + \varrho - rs\sigma - s - \sigma \quad \text{by (3. 2)} \\
&= s\sigma(\varrho - r) + \varrho - s - \sigma \\
&= \frac{1}{\varrho}(s\sigma + \varrho^2 - s\varrho - \sigma\varrho) \quad \text{by (3. 1)} \\
&= \frac{1}{\varrho}(1 + r\varrho + s\sigma - s\varrho - \sigma\varrho) \quad \text{by (3. 1)} \\
&> (1/\varrho)\,[1 + (\sigma - \varrho)^2 + r\sigma - \sigma\varrho] \quad \text{by lemma 1.} \\
&= (1/\varrho)\,[(\sigma - \varrho)^2 + 1 - (\sigma/\varrho)] \quad \text{by (3. 1)} \\
&= (1/\varrho)\,[(\sigma - \varrho)^2 - (\sigma - \varrho)/\varrho] \\
&= (1/\varrho)\,(\sigma - \varrho)\,[\sigma - \varrho - 1/\varrho] > 0
\end{aligned}$$

since $s \geqq r + 1$, and min $(\sigma - \varrho)$ occurs when $s = 2$, $r = 1$, with max $(1/\varrho)$ occuring when $r = 1$ and in this case we have (since $2 \cdot 4 < \sigma < 2 \cdot 5$, $1 \cdot 5 < \varrho < 1.67$),

$$\sigma - \varrho > 0.73 \qquad 1/\varrho < 0.67.$$

This disposes of the case when $i = 1$, so now we suppose $i \geqq 2$.

We note the following result for continuants, (see Good [1], p. 217),

$$\begin{aligned}
(3.\,7) \qquad & K(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m) \\
&= K(a_1, \ldots, a_n) \cdot K(b_1, \ldots, b_m) + K(a_1, \ldots, a_{n-1}) \cdot K(b_2, \ldots, b_m).
\end{aligned}$$

Now using (3. 4) with $u = i - 2$, $i - 3$, $(i \geqq 3)$, (3.5) and (3.6), we get from (3.7),

$$\begin{aligned}
(3.\,8) \qquad Q(u, v - 1) &\leqq A \cdot \varrho^{u-i+2} \cdot \sigma^{v-1} \left\{\frac{r}{\varrho}\left(\frac{r}{\varrho} + \frac{1}{\varrho\sigma}\right) + \frac{1}{\varrho^2}\right\} \left\{\frac{\varrho^i + (-\varrho)^{-i+2}}{1 + \varrho^2}\right\} \\
&\quad + A\varrho^{u-i+1} \cdot \sigma^{v-1} \left\{\frac{r}{\varrho} + \frac{1}{\varrho\sigma}\right\} \left\{\frac{\varrho^{i-1} + (-\varrho)^{-i+3}}{1 + \varrho^2}\right\}
\end{aligned}$$

(this also holds for $i = 2$, as may be verified directly). There is a corresponding result with $u - 1$ in place of u for $Q(u - 1, v - 1)$, and substituting this in equation (A) (iii) we have

$$\begin{aligned}
Q(u, v) &\leqq A\varrho^{u-i+2} \cdot \sigma^{v-1} \left[\frac{r}{\varrho}\left(\frac{r}{\varrho} + \frac{1}{\varrho\sigma}\right) + \frac{1}{\varrho^2}\right] \left[\frac{s\varrho^i + s(-\varrho)^{-i+2} + \varrho^{i-1} + (\varrho)^{-i+3}}{\varrho^2 + 1}\right] \\
&\quad + A\varrho^{u-i+1} \cdot \sigma^{v-1} \left[\frac{r}{\varrho} + \frac{1}{\varrho\sigma}\right] \left[\frac{s\varrho^{i-1} + s(-\varrho)^{-i+3} + \varrho^{i-2} + (-\varrho)^{-i+4}}{\varrho^2 + 1}\right] \\
&\leqq A \cdot \varrho^u \sigma^v \left\{\frac{(r^2\sigma + r + \sigma)\,[s\varrho^2 + \varrho + \varrho^{4-2i}(s - \varrho)] + (r\sigma + 1)\,[s\varrho + 1 - \varrho^{5-2i}(s - \varrho)]}{\varrho^2(\varrho^2 + 1)\,\sigma^2}\right\}.
\end{aligned}$$

The last step follows since $r^2\sigma + r + \sigma - r\varrho\sigma - \varrho > 0$, and so

$$(-1)^i \cdot [r^2\sigma + r + \sigma - r\varrho\sigma - \varrho] \leqq r^2\sigma + r + \sigma - r\varrho\sigma - \varrho.$$

Now we have to show that the expression in brackets is $\leqq 1$, i. e. if we denote it by N/D, then we have to show that $D - N \geqq 0$.

$$\begin{aligned}
N = (r^2\sigma + r + \sigma)\,(s\varrho^2 + \varrho) + (r\sigma + 1)\,(s\varrho + 1) \\
- \varrho^{-2i+4}(s - \varrho)(r\varrho\sigma + \varrho - r^2\sigma - r - \sigma).
\end{aligned}$$

Now

$$r\varrho\sigma + \varrho - r^2\sigma - r - \sigma = \frac{\sigma r}{\varrho} + \varrho - r - \sigma$$
$$= \sigma\left(\frac{r}{\varrho} - 1\right) + \varrho - r$$
$$= (\varrho - r)\left(1 - \frac{\sigma}{\varrho}\right)$$
$$= \frac{-(\sigma - \varrho)}{\varrho^2}$$

giving

$$N = \varrho^2 r^2 \sigma s + \varrho^2 rs + \varrho^2 \sigma s + \varrho r^2 \sigma + \varrho r + \varrho\sigma + \varrho r\sigma s + r\sigma + \varrho s + 1 + \varrho^{-2i+2}(s-\varrho)(\sigma-\varrho),$$
$$D = (\varrho^2 + 1)\,\varrho^2\sigma^2 = \varrho^2 r^2 \sigma s + 3\varrho r\sigma s + 2\sigma s + \varrho^2 r^2 + 3\varrho r + 2,$$
$$D - N = 2\varrho r\sigma s + 2\sigma s + \varrho^2 r^2 + 2\varrho r + 1 - \varrho^2 rs - \varrho^2\sigma s - \varrho r^2\sigma - \sigma\varrho$$
$$- r\sigma - \varrho s - \varrho^{-2i+2}(s-\varrho)(\sigma-\varrho)$$
$$= \varrho^2\sigma s + \varrho^2 r^2 + 2\varrho r + 1 - \varrho^2 rs - \varrho r^2\sigma - \varrho\sigma - r\sigma - \varrho s - \varrho^{-2i+2}(s-\varrho)(\sigma-\varrho)$$
$$= \varrho^2(\sigma s + r^2 - rs - r\sigma) + 2\varrho r + 1 - \varrho\sigma - \varrho s - \varrho^{-2i+2}(s-\varrho)(\sigma-\varrho)$$
$$= \varrho^2(s-r)(\sigma-r) - \varrho(\sigma-r) - \varrho(s-r) + 1 - \varrho^{-2i+2}(s-\varrho)(\sigma-\varrho),$$

$$(3.9)\quad D - N \geqq (s-r)(\sigma-r)\left[\varrho^2 - \varrho\left(\frac{1}{s-r} + \frac{1}{\sigma-r}\right) - \varrho^{-2i+2}\right] + 1$$
$$\geqq (s-r)(\sigma-r)(\varrho^2 - 2\varrho - 1) + 1 > 0$$

for $r \geqq 2$, since $s - r \geqq 1$, $\sigma - r > 1$ and $\varrho^{-2i+2} < 1$ for $i \geqq 2$.

When $r = 1$ we consider the inequality (3. 9), where if $s \geqq 3$,

$$\left(\frac{1}{s-r} + \frac{1}{\sigma-r}\right) < 1$$

giving

$$D - N \geqq (s-r)(\sigma-r)(\varrho^2 - \varrho - 1) + 1 > 0.$$

The only case left is when $r = 1$, $s = 2$. We note that $i \geqq 2$, so $\varrho^{-2i+2} \leqq \varrho^2$, and substituting these values in (3. 9) gives

$$D - N \geqq (\sigma - 1)\,\varrho^2 - (\sigma - 1)\,\varrho - \varrho - (\sigma - 1)/\varrho^2 + 1$$
$$= (\sigma - 1) - \varrho - (\sigma - 1)/\varrho^2 + 1$$
$$= \sigma - \varrho - (\sigma - 1)/\varrho^2 > 0.73 - 1.5/(1.5)^2 > 0$$

by the values given previously.

This completes the proof of theorem 2.

4. Application to fractional dimension.

We shall now use the above results in theorem G, with d in place of τ, $\alpha_1 = r$, $\alpha_2 = s$. We note that there are $\binom{u+v}{v}$ different $Q(u, v)$ for fixed u and v, so when $u + v = n$, we have

$$A_1 \sum_{v=0}^{n} \binom{n}{v} r^{-2ud} s^{-2vd} \geqq \sum K(a_1, \ldots, a_n)^{-2d} \geqq A_2 \sum_{v=0}^{n} \binom{n}{v} \varrho^{-2ud} \sigma^{-2vd},$$

that is

$$A_1(r^{-2d} + s^{-2d})^n \geqq \sum K(a_1, \ldots, a_n)^{-2d} \geqq A_2(\varrho^{-2d} + \sigma^{-2d})^n.$$

Let us take the n'th root of these inequalities, then if d satisfies theorem G (i. e. τ in the theorem),

$$\left(\Sigma K(a_1, \ldots, a_n)^{-2d}\right)^{\frac{1}{n}} \to 1 \text{ as } n \to \infty.$$

Thus we obtain the inequalities

$$r^{-2d} + s^{-2d} \geqq 1, \tag{4. 1}$$

$$\varrho^{-2d} + \sigma^{-2d} \leqq 1. \tag{4. 2}$$

So if we denote by $E(r, s)$ the set of numbers represented by continued fractions whose partial quotients only contain r and s then we have the following result:

Theorem 3. *If* $\dim E(r, s) = d$, *then* $d_1 \leqq d \leqq d_2$, *where* d_1 *is the real root of*

$$r^{-2x} + s^{-2x} = 1,$$

and d_2 *the real root of*

$$\varrho^{-2x} + \sigma^{-2x} = 1$$

where $\varrho = (1/2)\,(r + \sqrt{r^2 + 4})$, $\sigma = (1/2)\,(s + \sqrt{s^2 + 4})$.

5. Notes.

In theorem 2 the result can not be improved in the form given, since there are $Q(u, v)$ which do reach the order of magnitude given. To try to improve the result given by similar methods would mean considering the order of the partial quotients and this leads to heavy algebra.

Theorem 2 suggests a similar result with three or more integers, but this would mean eight equations in place of the four in (A), so I have not considered it. But I think that the result is very likely to be true, in which case it would lead to extensions of theorem 3. Theorem 1 can easily be extended in this way, and here it is probably possible to improve the approximation given by a geometric order.

In theorem 3 it is a fairly obvious corollary that $d_1 - d_2 \to 0$ as r and $s \to \infty$, but since each root tends to zero this does not prove much. In fact by considering

$$f(x, y, z) = x^{-2x} + y^{-2}$$

and its differential we can show that $(d_2 - d_1)/d \to 0$ as r and $s \to \infty$.

These results arose from trying to find $\dim E(1, 2)$, at the suggestion of Professor Besicovich, but they do not give any more than is known in this problem.

Finally I should like to thank Dr. Volkmann for his interest in these results and for his suggestion to write them as a paper. Also I should like to thank him for his suggestions with regard to shortening the proof of theorem 2.

Reference.

1. *I. J. Good*, The fractional dimensional theory of continued fractions. Proc. Camb. Phil. Soc. (1941) Vol. 37, pp. 199 to 228.

Trinity College, Cambridge, and University of Western Ontario, London, Canada.

Eingegangen 31. März 1954, in revidierter Fassung am 1. Juli 1954.

Zum Waringschen Problem für algebraische Zahlen und Polynome.

Meinem verehrten Lehrer J. E. Hofmann zum 55. Geburtstag am 7. 3. 1955.

Von *G. J. Rieger* in Gießen.

Herr Kamke [4] hat 1921 in seiner Habilitationsschrift u. a. die folgenden zwei Sätze bewiesen.

Satz 1. *Zu jeder natürlichen Zahl n gibt es eine natürliche Zahl $N_1 = N_1(n)$ von folgender Art: Es sei K ein algebraischer Zahlkörper und*

$$\varphi(x) = \sum_{\nu=0}^{n} \alpha_\nu x^{n-\nu}$$

ein Polynom n-ten Grades mit $\alpha_\nu \in K$ $(\nu = 0, 1, \ldots, n)$, mit $\alpha_0 > 0$[1]*) und mindestens einer reellen Nullstelle in jedem reellen der konjugierten Körper*[2]*). Es bezeichne $u^{(i)}$ die größte Nullstelle im konjugierten Körper $K^{(i)}$, sofern dieser reell ist. Dann ist für jede Zahl $\xi > 0$ aus K die Gleichung*

$$\xi = \sum_{\varkappa=1}^{N_1} \varphi(\xi_\varkappa)$$

durch solche $\xi_\varkappa$ aus K lösbar, für welche in den reellen Körpern $K^{(i)}$[2]*)*

$$\xi_\varkappa^{(i)} > u^{(i)}$$

ist, also die Zahlen $\varphi(\xi_\varkappa) > 0$ sind.

Hierin ist für $\varphi(x) = x^n$ ein Satz von Herrn Siegel [6], für den Körper der rationalen Zahlen ein früherer Satz von Herrn Kamke [3] enthalten.

Satz 2. *Zu jeder natürlichen Zahl n gibt es eine natürliche Zahl $N_2 = N_2(n)$ von folgender Art: Ist $\gamma(x)$ eine definite rationale rationalzahlige Funktion*[3]*) vom Grad $m = \mu n$ (μ gerade, $\gtreqless 0$), so gibt es N_2 rationale rationalzahlige Funktionen $\xi_\varkappa(x)$ mit nirgends verschwindenden Nennern, so daß*

$$\gamma(x) = \sum_{\varkappa=1}^{N_2} \xi_\varkappa^n(x), \quad \xi_\varkappa(x) \geqq 0$$

ist.

Das Ziel der vorliegenden Arbeit ist es, N_1 und N_2 auf vollständig elementarem Wege durch n allein nach oben abzuschätzen. Das gelingt mit der gleichen Methode, die

---

[1]) Sind α, β Zahlen des Körpers, so soll $\alpha > \beta$ bedeuten, daß in allen reellen der konjugierten Körper $K^{(i)}$ die Ungleichung $\alpha^{(i)} > \beta^{(i)}$ besteht. Ist kein reeller unter den konjugierten Körpern vorhanden, d. h. ist K total imaginär, so wird durch $\alpha > \beta$ nichts ausgesagt.

[2]) Wenn K total imaginär ist, fällt diese Bedingung weg; ebenso die Ungleichung $\xi_\varkappa^{(i)} > u^{(i)}$.

[3]) Ein Polynom heißt rationalzahlig, wenn die Koeffizienten rationale Zahlen sind. Eine rationale Funktion heißt rationalzahlig, wenn sie als Quotient zweier rationalzahliger Polynome geschrieben werden kann. Eine rationale Funktion heißt hier definit, wenn sie stets > 0 ist und ihr Nenner nirgends verschwindet.

in meiner Dissertation [5] zu einer Abschätzung von $g(n)$ in der Hilbertschen Lösung des Waringschen Problems [1] geführt hat. Damit war die Funktion $g(n)$ erstmals auf elementarem Weg durch n allein nach oben abgeschätzt. § 1 und § 3 von [5] treten hier als § 1 und § 2 auf. In § 3 geben wir ein Lemma von Herrn Kamke wieder. In § 4 werden wir dann

$$N_1 = N_1(n) < (2n+3)^{3(2n+3)^9}$$

und

$$N_2 = N_2(n) < (2n+3)^{3(2n+3)^{11}}$$

beweisen.

In [7], [8] hat Herr Siegel 1944 das analoge Problem zu Satz 1 für total positive, *ganze* algebraische Zahlen behandelt und mit der Methode der „singular series" ein sehr scharfes Ergebnis erzielt. Allerdings hängt die dabei gefundene Schranke für die $N_1(n)$ entsprechende Größe vom Grad n des Polynoms $\varphi(x) = x^n$ und außerdem vom Grad des algebraischen Zahlkörpers K ab, in dem sich alles abspielt. Ob in diesem Falle eine Abschätzung durch n allein möglich ist, ist bis heute noch nicht bekannt. Nur für $n = 2$ ist das bisher gezeigt worden.

An dieser Stelle möchte ich der Studienstiftung des Deutschen Volkes für jahrelange Förderung herzlich danken.

§ 1. Das Lemma von Hilbert [4]).

Lemma 1. *Sind k, l beliebige natürliche Zahlen, so gilt in den Veränderlichen $x_1, \ldots, x_l$ eine Identität der Gestalt*

$$(1) \qquad (x_1^2 + \cdots + x_l^2)^k = \sum_{\mu=1}^{M} s_\mu (b_{\mu 1} x_1 + \cdots + b_{\mu l} x_l)^{2k};$$

dabei sind $M = M(k, l)$ eine natürliche Zahl, $s_\mu = s_\mu(k, l)$ positive rationale Zahlen, $b_{\mu\lambda} = b_{\mu\lambda}(k, l)$ ganze Zahlen $\neq 0$.

Beweis (nach E. Stridsberg [9]). Wir führen symbolische Potenzen

$$(2) \qquad h_i^{2k} = \frac{(2k)!}{k!}, \quad h_i^{2k+1} = 0 \qquad \begin{pmatrix} i = 1, 2, \ldots, l \\ k = 0, 1, 2, \ldots \end{pmatrix}$$

ein und erklären ein symbolisches Produkt

$$h_i^{k_1} \cdot h_i^{k_2} = h_i^{k_1 + k_2} \qquad \begin{pmatrix} i = 1, 2, \ldots, l \\ k_1, k_2 = 0, 1, 2, \ldots \end{pmatrix}.$$

Unter

$$h_i^{k_1} \cdot h_j^{k_2} \qquad \begin{pmatrix} i \neq j \\ i, j = 1, 2, \ldots, l \\ k_1, k_2 = 0, 1, 2, \ldots \end{pmatrix}$$

verstehen wir dagegen das gewöhnliche Produkt der beiden Zahlen $h_i^{k_1}$ und $h_j^{k_2}$.

Setzen wir nun $h_i^\varkappa = h_j^\varkappa = h^\varkappa$, so folgen die Identitäten

$$(3) \qquad \begin{aligned} (h_1 x_1 + \cdots + h_l x_l)^{2k} &= h^{2k}(x_1^2 + \cdots x_l^2)^k, \\ (h_1 x_1 + \cdots + h_l x_l)^{2k+1} &= 0. \end{aligned}$$

---

[4]) Vgl. [1], S. 283.

Sind $\beta_1, \ldots, \beta_m$ voneinander verschiedene reelle Zahlen, so sind durch das Gleichungssystem

$$(4) \qquad \sum_{\mu=1}^{m} \varrho_\mu \beta_\mu^\nu = h^\nu \qquad (\nu = 0, 1, \ldots, m-1)$$

die Zahlen ϱ_μ eindeutig bestimmt, da die Determinante gleich

$$\prod_{i>j} (\beta_i - \beta_j)$$

und damit $\neq 0$ ist.

Es besteht nun folgende Identität

$$(5) \qquad (h_1 x_1 + \cdots + h_l x_l)^k = \sum_{\mu_1, \ldots, \mu_l = 1}^{m} \varrho_{\mu_1} \cdots \varrho_{\mu_l} (\beta_{\mu_1} x_1 + \cdots + \beta_{\mu_l} x_l)^k \qquad (k = 0, 1, \ldots, m-1);$$

denn der Koeffizientenvergleich liefert

$$\frac{k!}{k_1! \cdots k_l!} h_1^{k_1} \cdots h_l^{k_l} = \frac{k!}{k_1! \cdots k_l!} \sum_{\mu_1, \ldots, \mu_l = 1}^{m} \varrho_{\mu_1} \cdots \varrho_{\mu_l} \beta_{\mu_1}^{k_1} \cdots \beta_{\mu_l}^{k_l} \left(\begin{matrix} k_\lambda \geqq 0 \\ \sum_{\lambda=1}^{l} k_\lambda = k \end{matrix} \right);$$

das aber ist eine unmittelbare Folge von (4).

Wählen wir $\beta_1, \ldots, \beta_m$ als Nullstellen gewisser Polynome $H_m(x)$, so können wir zeigen, daß alle ϱ_μ positiv ausfallen.

Dazu setzen wir in (3)

$$l = 2, \; x_1 = x + 1, \; x_2 = i, \; k = m$$

und erhalten

$$(hx + h + h_1 i)^{2m} = \frac{(2m)!}{m!} x^m (x+2)^m,$$
$$(hx + h + h_1 i)^{2m+1} = 0.$$

Daraus folgt durch Koeffizientenvergleich

$$(6) \qquad \begin{aligned} h^\mu (h + h_1 i)^\nu &= 0 \qquad (\mu < \nu), \\ h^m (h + h_1 i)^m &= m!\, 2^m. \end{aligned}$$

Wir definieren jetzt die Polynome

$$H_m(x) = (x + hi)^m$$
$$= \sum_{\mu=0}^{\left[\frac{m}{2}\right]} (-1)^\mu \binom{m}{2\mu} h^{2\mu} x^{m-2\mu} = \sum_{\mu=0}^{\left[\frac{m}{2}\right]} (-1)^\mu \frac{m!}{\mu!\,(m-2\mu)!} x^{m-2\mu}.$$

Für sie gilt

$$H_m(x) = x H_{m-1}(x) - 2(m-1) H_{m-2}(x),$$
$$H'_m(x) = m \cdot H_{m-1}(x).$$

Die Polynome $H_m(x), H_{m-1}(x), \ldots, H_0(x) = 1$ bilden eine Sturmsche Kette für das Intervall $(-\infty, +\infty)$. Nach bekannten Sätzen (vgl. etwa O. Perron, Algebra I) sind alle Nullstellen von $H_m(x)$ reell und voneinander verschieden: $\beta_1, \ldots, \beta_m$.

Wir setzen

$$\frac{H_m(x)}{x - \beta_\pi} = H_{m,\pi}(x) \qquad (\pi = 1, \ldots, m).$$

Dann ist

$$(7)\qquad \begin{aligned} H_{m,\pi}(\beta_\mu) &= 0 && (\mu \neq \pi),\\ H_{m,\pi}(\beta_\pi) &= H'_m(\beta_\pi) = mH_{m-1}(\beta_\pi) \neq 0. \end{aligned}$$

Es sei nun

$$\varphi_n(x) = \sum_{\nu=0}^{n} a_\nu x^{n-\nu}.$$

Aus (6) folgt

$$(8)\qquad \begin{aligned} \varphi_n(h)\, H_m(h) &= 0 && (n < m),\\ \varphi_m(h)\, H_m(h) &= a_0 h^m H_m(h) = a_0 m!\, 2^m. \end{aligned}$$

$\varphi_n(x)$ sei vom Grad $n \leqq m$. Dann folgt

$$\varphi_n(x) - \varphi_n(\beta_\pi) = (x - \beta_\pi)\, \psi_{n-1}(x)$$

und daraus nach (7), (8)

$$(\varphi_n(h) - \varphi_n(\beta_\pi))\, H_{m,\pi}(h) = \psi_{n-1}(h) \cdot H_m(h) = 0$$

und daraus

$$(9)\qquad \varphi_n(h)\, H_{m,\pi}(h) = \varphi_n(\beta_\pi)\, H_{m,\pi}(h) \qquad (n \leqq m).$$

Aus (8), (9) folgt

$$(10)\qquad (m-1)!\, 2^{m-1} = H_{m-1}(h)\, H_{m,\pi}(h) = H_{m-1}(\beta_\pi)\, H_{m,\pi}(h).$$

Ist $\varphi_n(x)$ ein beliebiges Polynom von einem Grad $n < m$, so kann man stets schreiben

$$(11)\qquad \varphi_n(x+h) = \sum_{\mu=1}^{m} \varrho_\mu\, \varphi_n(x + \beta_\mu);$$

denn für das Bestehen dieser Identität ist offenbar hinreichend, daß

$$a_{n-\varkappa}(x+h)^\varkappa = \sum_{\mu=1}^{m} \varrho_\mu a_{n-\varkappa}(x+\beta_\mu)^\varkappa \qquad (0 \leqq \varkappa \leqq n)$$

ist. Diese neue Identität ist aber richtig, denn durch Koeffizientenvergleich erhalten wir die Aussage (4).

Aus (10), (11), (7) folgt

$$(12)\quad (m-1)!\, 2^{m-1} = H_{m-1}(\beta_\pi)\, H_{m,\pi}(h) = H_{m-1}(\beta_\pi) \sum_{\mu=1}^{m} \varrho_\mu H_{m,\pi}(\beta_\mu) = \varrho_\pi m H^2_{m-1}(\beta_\pi).$$

Also ist

$$\varrho_\pi > 0 \qquad (\pi = 1, 2, \ldots, m).$$

Wir ersetzen nun die reellen Zahlen $\beta_1, \ldots, \beta_m$ durch die rationalen $\beta'_1, \ldots, \beta'_m$, die so nahe bei den Zahlen $\beta_1, \ldots, \beta_m$ liegen, daß alle Lösungen ϱ'_μ des Gleichungssystems

$$(13)\qquad \sum_{\mu=1}^{m} \varrho'_\mu \beta'^\nu_\mu = h^\nu \qquad (\nu = 0, 1, \ldots, m-1)$$

größer als Null bleiben. Das ist möglich, da die Lösungen des Gleichungssystems (4) stetig von den Koeffizienten abhängen. Die ϱ'_μ sind als Lösungen eines linearen Gleichungssystems mit rationalen Koeffizienten sicher auch rational.

Im Hinblick auf die späteren Überlegungen ist es zweckmäßig, zusätzlich $\beta'_1, \ldots, \beta'_m$ ungleich Null zu verlangen. Wegen der Beziehung

$$H_m(-x) = (-1)^m H_m(x)$$

liegen die Nullstellen von $H_m(x)$ symmetrisch zum Ursprung. Offenbar ist die Bedingung

$$0 < \beta'_\pi - \beta_\pi < \tfrac{1}{2} \min_{\mu \neq \nu} |\beta_\mu - \beta_\nu| \qquad (\pi, \mu, \nu = 1, \ldots, m) \tag{14}$$

hinreichend ist für $\beta'_\pi \neq 0$.

Wir schreiben jetzt (5) in den gestrichenen Größen für den Exponenten $2k$ auf $(2k < m)$, setzen das mit (3) zusammen und ziehen noch den Hauptnenner aus den Klammern $(\beta'_{\mu_1} x_1 + \cdots + \beta'_{\mu_l} x_l)$ heraus. Damit erhalten wir die Aussage (1) des Lemmas

$$\begin{aligned} (x_1^2 + \cdots + x_l^2)^k &= \frac{1}{h^{2k}} \sum_{\mu_1, \ldots, \mu_l = 1}^{m} \varrho'_{\mu_1} \cdots \varrho'_{\mu_l} (\beta'_{\mu_1} x_1 + \cdots + \beta'_{\mu_l} x_l)^{2k} \\ &= \sum_{\mu=1}^{M} s_\mu(k, l) (b_{\mu 1} x_1 + \cdots + b_{\mu l} x_l)^{2k} \qquad (2k < m). \end{aligned} \tag{15}$$

Nach Vorgabe von k wählen wir zweckmäßig

$$m = 2k + 1. \tag{16}$$

Offenbar ist in (15)

$$M = M(k, l) = m^l = (2k + 1)^l; \tag{17}$$

die $s_\mu(k, l)$ sind sicher rational und positiv, da die $\varrho'_{\mu\lambda}$ rational und positiv sind; die $b_{\mu\lambda}(k, l)$ sind ganz und wegen $\beta'_\pi \neq 0$ ist auch

$$b_{\mu\lambda}(k, l) \neq 0. \tag{18}$$

Damit ist das Lemma von Hilbert vollständig bewiesen.

§ 2. Abschätzungen zum Lemma von Hilbert.

Wir haben eben gesehen, daß die $s_\mu(k, l)$ in (1) rationale Zahlen sind:

$$s_\mu(k, l) = \frac{u_\mu(k, l)}{v_\mu(k, l)}. \tag{19}$$

Dabei — und das gilt für alle hier auftretenden rationalen Zahlen — sind die u_μ, v_μ ganze Zahlen mit $v_\mu > 0$ und $(u_\mu, v_\mu) = 1$.

Wir streben jetzt eine obere Abschätzung für $v_\mu(k, l)$ an. Das gelingt auf folgendem Wege:

Bezeichnen wir die m Nullstellen von $H_m(x)$ mit $\beta_\mu(m)$, so werden wir aus einer Abschätzung von $|\beta_\mu(m)|$ nach oben vermittels (12) eine Abschätzung

$$\varrho_\pi > \varrho(m) \text{ mit } \varrho(m) > 0 \qquad (\mu, \pi = 1, \ldots, m)$$

herleiten. Wir ersetzen dann die β_μ, die rational oder irrational sein können, durch benachbarte rationale Zahlen $\beta'_\mu > \beta_\mu$. Dadurch gehen vermöge (4) bzw. (13) die reellen Zahlen ϱ_π in die rationalen ϱ'_π über. Man kann nun eine natürliche Zahl $N_0(m)$ so finden, daß aus

$$\beta'_\mu - \beta_\mu \leqq \frac{1}{N_0(m)} = b(m) \qquad (\mu = 1, \ldots, m)$$

die Abschätzung

$$|\varrho'_\pi - \varrho_\pi| < \varrho(m) \qquad (\pi = 1, \ldots, m),$$

folgt, was offenbar hinreichend ist für $\varrho'_\pi > 0$, wie wir es haben wollen.

Nun liegt bekanntlich in einem halboffenen Intervall der Länge $\frac{1}{N_0}$, wobei N_0 eine natürliche Zahl ist, genau eine rationale Zahl mit einem Nenner, der Teiler von N_0 ist. Wir können die β'_μ also mit der folgenden Eigenschaft wählen:

(20) Alle β'_μ haben $N_0(m)$ oder einen Teiler davon als Nenner.

Ist $N'_0(m)$ eine noch näher zu bestimmende obere Schranke für die Nenner der ϱ'_π, so ergibt sich sofort wegen (19), (15), (16)

$$(21)\quad v_\mu(k,l) \leqq \frac{(2k)!}{k!} \cdot N_0(m)^l \cdot N_0(m)^{2k} = \frac{(2k)!}{k!} \cdot N'_0(2k+1)^l \cdot N_0(2k+1)^{2k}.$$

Im einzelnen bleibt uns nur noch übrig, $|\beta_\mu(m)|$ nach oben und $\varrho(m)$ nach unten abzuschätzen. Danach werden wir mit Hilfe einiger Determinantenabschätzungen $N_0(m)$ bestimmen. Daraus ergibt sich sofort $N'_0(m)$; damit ist dann durch die Formel (21) eine obere Abschätzung von $v_\mu(k,l)$ durch k, l allein gewonnen. Wir müssen jetzt nur noch zusehen, daß (14) erfüllt wird.

Auf ähnliche Weise wie die $v_\mu(k,l)$ lassen sich auch die $b_{\mu\lambda}(k,l)$ abschätzen.

Wegen (16) können wir für das folgende stets $m \geqq 3$ annehmen.

1. Bei den Polynomen

$$H_m(x) = (x+hi)^m = \sum_{\mu=0}^{\left[\frac{m}{2}\right]} (-1)^\mu \frac{m!}{\mu!(m-2\mu)!} x^{m-2\mu}$$

alternieren die Vorzeichen. Aus $x \geqq m - \frac{1}{2}$ folgt

$$\frac{m!}{(2\mu)!(m-4\mu)!} x^{m-4\mu} > \frac{m!}{(2\mu+1)!(m-4\mu-2)!} x^{m-4\mu-2} \quad (2 \leqq 4\mu+2 \leqq m);$$

also hat jedes Glied mit dem positiven Vorzeichen einen größeren Betrag als das nachfolgende Glied, das ja negatives Vorzeichen hat. Aus $x \geqq m - \frac{1}{2}$ folgt also $H_m(x) > 0$. Berücksichtigen wir noch, daß wegen

$$H_m(-x) = (-1)^m H_m(x)$$

die Nullstellen symmetrisch zum Ursprung liegen, so ergibt sich

$$(22)\qquad |\beta_\mu(m)| < m - \tfrac{1}{2} \qquad (\mu = 1, \ldots, m).$$

Daraus folgt nun wegen

$$m^2 \cdot \frac{(m-1)!}{\mu!(m-1-2\mu)!} > \frac{(m-1)!}{(\mu+1)!(m-1-2\mu-2)!} \quad \left(1 \leqq \mu+1 \leqq \frac{m-1}{2}\right)$$

die Abschätzung

$$|H_{m-1}(\beta_\lambda)| \leqq \sum_{\mu=0}^{\left[\frac{m-1}{2}\right]} \frac{(m-1)!\,|\beta_\lambda|^{m-1-2\mu}}{\mu!(m-1-2\mu)!} < \sum_{\mu=0}^{\left[\frac{m-1}{2}\right]} \frac{(m-1)!\,m^{m-1-2\mu}}{\mu!(m-1-2\mu)!}$$
$$\leqq \left(\frac{m-1}{2}+1\right) m^{m-1} < m^m \qquad (\lambda = 1, \ldots, m).$$

Setzen wir das in (12) ein, so folgt

$$(23)\qquad \varrho_\pi > \varrho(m) = \frac{2^{m-1}(m-1)!}{m^{2m+1}} \qquad (\pi = 1, \ldots, m).$$

2. Nun folgen einige Determinantenabschätzungen. Wir verwenden dabei die Vektorschreibweise. Es sei

$$\mathfrak{a}_i = (a_{i1}, \ldots, a_{in}), \qquad \mathfrak{a}'_i = (a'_{i1}, \ldots, a'_{in}), \qquad \mathfrak{e}_i = (e_{i1}, \ldots, e_{in}),$$

$$A = \begin{vmatrix} \mathfrak{a}_1 \\ \cdot \\ \cdot \\ \cdot \\ \mathfrak{a}_n \end{vmatrix}, \qquad A' = \begin{vmatrix} \mathfrak{a}'_1 \\ \cdot \\ \cdot \\ \cdot \\ \mathfrak{a}'_n \end{vmatrix}$$

und

$$a'_{ik} = a_{ik} + e_{ik} \qquad (i, k = 1, \ldots, n).$$

Dann ist offenbar

$$A' = A + \sum_{i=1}^{n} \begin{vmatrix} \mathfrak{a}_1 \\ \cdot \\ \cdot \\ \mathfrak{a}_{i-1} \\ \mathfrak{e}_i \\ \mathfrak{a}'_{i+1} \\ \cdot \\ \cdot \\ \mathfrak{a}'_n \end{vmatrix} = A + \sum_{i,k=1}^{n} e_{ik} A^*_{ik} \tag{24}$$

mit

$$A^*_{ik} = (-1)^{i+k} \begin{vmatrix} a_{11} & \cdots & a_{1\,k-1} & a_{1\,k+1} & \cdots & a_{1n} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ a_{i-1\,1} & \cdots & a_{i-1\,k-1} & a_{i-1\,k+1} & \cdots & a_{i-1\,n} \\ a'_{i+1\,1} & \cdots & a'_{i+1\,k+1} & a'_{i+1\,k+1} & \cdots & a'_{i+1\,n} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ a'_{n1} & \cdots & a'_{n\,k-1} & a'_{n\,k+1} & \cdots & a'_{nn} \end{vmatrix}.$$

Eine rohe Abschätzung liefert

$$|A| \leqq n! \prod_{i=1}^{n} \left(\max_{k=1}^{n} |a_{ik}| \right). \tag{25}$$

3. Jetzt schätzen wir $|\varrho'_k - \varrho_k|$ mit Hilfe dieser allgemeinen Determinantenabschätzungen nach oben ab. An Stelle von A wählen wir

$$\begin{vmatrix} \beta_1^0 & \cdots & \beta_m^0 \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \beta_1^{m-1} & \cdots & \beta_m^{m-1} \end{vmatrix} = \prod_{\mu > \nu} (\beta_\mu - \beta_\nu) = B,$$

die Determinante des Gleichungssystems (4). Durch Streichen der Zeile i und der Spalte k und Multiplikation mit $(-1)^{i+k}$ entsteht die Adjunkte B_{ik}, bis auf das Vorzeichen eine $(m-1)$-reihige Unterdeterminante. Aus (4) folgt

$$\varrho_k = \sum_{i=1}^{m} h^{i-1} \frac{B_{ik}}{B} \qquad (k = 1, \ldots, m).$$

Wir ersetzen jetzt β_k durch

$$\beta'_k = \beta_k + b_k \qquad (k = 1, \ldots, m)$$

mit

$$0 < b_k \leqq b \text{ [5]}.$$

---

[5]) **Durch die Forderung $b_k > 0$ haben wir bereits den einen Teil der Bedingung (14) berücksichtigt.**

Dabei gehen B, B_{ik}, ϱ_k in B', B'_{ik}, ϱ'_k über. Es ist

$$\varrho'_k - \varrho_k = \sum_{i=1}^{m} h^{i-1}\left(\frac{B'_{ik}}{B'} - \frac{B_{ik}}{B}\right) = \sum_{i=1}^{m} h^{i-1}\left(\frac{B'_{ik} - B_{ik}}{B} + \frac{B'_{ik}}{BB'}(B - B')\right).$$

Also ist

$$(26) \quad |\varrho'_k - \varrho_k| \leqq \frac{1}{|B|}\left(\sum_{i=1}^{m} h^{i-1}\,|B'_{ik} - B_{ik}| + \frac{|B - B'|}{|B'|}\sum_{i=1}^{m} h^{i-1}\,|B'_{ik}|\right).$$

Nun werden die in (26) rechts stehenden Größen abgeschätzt.

a) Offenbar ist B^2 eine symmetrische Funktion der β_k. Der Hauptsatz über symmetrische Funktionen sagt aus:

Ist $S(\beta_1, \ldots, \beta_m)$ eine symmetrische Funktion mit Koeffizienten aus einem Ring $\mathfrak{R}$, so läßt sich die Funktion $S(\beta_1, \ldots, \beta_m)$ eindeutig als Polynom in den symmetrischen Grundfunktionen mit Koeffizienten aus $\mathfrak{R}$ darstellen.

Die symmetrischen Grundfunktionen der β_k sind in unserem Falle die Koeffizienten des Polynoms $H_m(x)$, also ganzrationale Zahlen. Also ist auch B^2 eine ganzrationale Zahl. Da B reell und $\neq 0$ ist, folgt

$$(27) \qquad |B| \geqq 1.$$

b) Wegen (24) ist

$$(28) \qquad |B'_{ik} - B_{ik}| \leqq \sum_{\substack{j \neq i \\ l \neq k}} |e_{jl} B^{*(jl)}_{ik}|;$$

dabei wird über j, l so summiert, daß

$$j \neq i,\ l \neq k;\quad j = 1, \ldots, m;\quad l = 1, \ldots, m$$

ist; ferner entspricht $B^{*(jl)}_{ik}$ der Determinante A^*_{jl}, wobei wir nur noch die Zeile i und die Spalte k streichen.

Offenbar ist wegen $\beta'_k > \beta_k$ und wegen der symmetrischen Lage der β_k auch

$$\beta' = \beta'(m) = \max_{k=1}^{m} |\beta'_k| > \beta = \beta(m) = \max_{k=1}^{m} |\beta_k|.$$

Wir setzen jetzt

$$(29) \qquad b \leqq \tfrac{1}{2}$$

voraus. Wegen (22) ist dann $\beta' < m$. Wir wenden (25) an und erhalten

$$B^{*(jl)}_{ik} < (m-2)!\ \beta'^{\binom{m}{2}-(i-1)-(j-1)} < (m-2)!\ m^{\binom{m}{2}-i-j+2}.$$

In unserem Falle ist $e_{jl} = (\beta_l + b_l)^{j-1} - \beta_l^{j-1}$ und daher

$$|e_{jl}| = |(\beta_l + b_l)^{j-1} - \beta_l^{j-1}| \leqq (\beta + b)^{j-1} - \beta^{j-1}.$$

Es ist

$$\beta < m \text{ wegen (22)},$$

$$\binom{m}{\nu} \leqq 2^{m-1},$$

$$b < \frac{m}{2} \text{ wegen (29)}.$$

Dann folgt für $j \geqq 2$

$$0 \leqq |e_{jl}| \leqq 2^{j-2} m^{j-2} b\left(1 + \frac{b}{m} + \left(\frac{b}{m}\right)^2 + \cdots\right) \leqq 2 \cdot 2^{j-2} m^{j-2} b.$$

Das gilt aber auch für $j = 1$, da $e_{1l} = 0$ ist. Somit geht (28) über in

$$|B'_{ik} - B_{ik}| < \sum_{\substack{j \neq i,1 \\ l \neq k}} 2^{j-1} m^{j-2} b \cdot (m-2)!\, m^{\binom{m}{2}-i-j+2};$$

dabei wird über j, l so summiert, daß

$$j \neq i, 1; \quad l \neq k; \quad j = 1, \ldots, m; \quad l = 1, \ldots, m$$

ist. Führen wir diese Summation aus, so folgt

$$|B'_{ik} - B_{ik}| < 2^m (m-1)!\, m^{\binom{m}{2}-i} b.$$

Wegen (2) ist

$$h^{i-1} \leqq (i-1)! \leqq (i-1)^{i-1} < m^{i-1} \qquad (i-1 < m).$$

Also folgt

$$\sum_{i=1}^{m} h^{i-1} |B'_{ik} - B_{ik}| < 2^m (m-1)!\, m^{\binom{m}{2}} b. \tag{30}$$

c) Durch Anwenden von (25) erhalten wir

$$|B'_{ik}| \leqq (m-1)!\, \beta'^{\binom{m}{2}-i+1} < (m-1)!\, m^{\binom{m}{2}-i+1},$$

$$\sum_{i=1}^{m} h^{i-1} |B'_{ik}| \leqq \sum_{i=1}^{m} (m-1)!\, m^{\binom{m}{2}-i+1+i-1} = (m-1)!\, m^{\binom{m}{2}+1}. \tag{31}$$

d) Durch Anwenden von (24) erhalten wir

$$\begin{aligned} |B' - B| &\leqq \sum_{i,k} |e_{ik} B^*_{ik}| < \sum_{i,k} 2^{i-1} \beta^{i-2} b \cdot (m-1)!\, \beta'^{\binom{m}{2}-i+1} \\ &< \sum_{i,k} 2^{i-1} b (m-1)!\, \beta'^{\binom{m}{2}-1} < 2^m m!\, m^{\binom{m}{2}-1} b \leqq \tfrac{1}{2}. \end{aligned} \tag{32}$$

Wir setzen über b also voraus, daß

$$2^m m!\, m^{\binom{m}{2}-1} b \leqq \tfrac{1}{2} \tag{33}$$

ist. Dann ist wegen (27) sicher

$$|B'| = \prod_{\mu > \nu} |\beta'_\mu - \beta'_\nu| \geqq \tfrac{1}{2} \tag{34}$$

und damit auch

$$\beta'_\mu \neq \beta'_\nu \qquad (\mu \neq \nu).$$

Aus (26), (27), (30), (31), (32), (34) folgt

$$\begin{aligned} |\varrho'_k - \varrho_k| &\leqq 2^m (m-1)!\, m^{\binom{m}{2}} b + 2 \cdot 2^m m!\, m^{\binom{m}{2}-1} b (m-1)!\, m^{\binom{m}{2}+1} \\ &< 2^{m+2} (m!)^2 m^{m^2-m-1} b. \end{aligned}$$

4. Wir werden jetzt noch bewirken, daß

$$|\varrho'_k - \varrho_k| < \varrho(m)$$

wird. Dafür ist wegen (23) hinreichend, daß

$$2^{m+2} (m!)^2 m^{m^2-m-1} b \leqq \frac{2^{m-1}(m-1)!}{m^{2m+1}}$$

oder

$$(35) \qquad b \leqq \frac{1}{8m!\, m^{m^2+m+1}} = \frac{1}{N_0(m)}$$

ist. Diese endgültige Bedingung für b enthält alle vorausgegangenen: (29) und (33). Sie sorgt auch dafür, daß die noch zu berücksichtigende rechte Seite von (14) erfüllt wird; denn wegen

$$B = \prod_{\mu > \nu} (\beta_\mu - \beta_\nu), \quad |B| \geqq 1, \quad \beta < m$$

ist

$$1 \leqq |B| \leqq \min_{\mu \neq \nu} |\beta_\mu - \beta_\nu| \cdot (2\beta)^{\binom{m}{2}-1}$$

oder

$$\min_{\mu \neq \nu} |\beta_\mu - \beta_\nu| \geqq (2m)^{1-\binom{m}{2}},$$

was wegen (35) offenbar $> 2b$ ist.

5. Wegen (20) ist auch B'_{ik} eine rationale Zahl und hat als Nenner die Zahl

$$N_0^{\binom{m}{2}-(i-1)}$$

oder einen Teiler davon; das gilt für $k = 1, \ldots, m$.

Offenbar hat $|\beta'_\mu - \beta'_\nu|$ als Nenner die Zahl $N_0(m)$ oder einen Teiler davon und damit einen Zähler $\leqq 2\beta' N_0(m)$. Auch $B' = \prod_{\mu > \nu} (\beta'_\mu - \beta'_\nu)$ ist eine rationale Zahl und hat als Zähler eine (ganze) Zahl D, für die sicher

$$D \leqq (2\beta' N_0)^{\binom{m}{2}}$$

gilt. Weil der Hauptnenner von

$$\sum_{i=1}^{m} h^{i-1} B'_{ik}$$

entweder gleich $N_0^{\binom{m}{2}}$ oder ein Teiler davon ist, gilt für den Nenner R_k von

$$\varrho'_k = \frac{1}{B'} \sum_{i=1}^{m} h^{i-1} B'_{ik}$$

sicher

$$R_k \mid D \cdot N_0^{\binom{m}{2}} \qquad (k = 1, \ldots, m),$$

also insbesondere

$$R_k \leqq D \cdot N_0^{\binom{m}{2}} \leqq (2\beta' N_0)^{\binom{m}{2}} \cdot N_0^{\binom{m}{2}} = N'_0(m).$$

Nun ist aber

$$8m! < m^{m+1} \text{ wegen } m \geqq 3.$$

Damit folgt aus (35)

$$(36) \qquad \begin{aligned} N_0(m) &< m^{m^2+2m+2}, \\ N_0(2k+1) &< (2k+1)^{4k^2+6k+5}. \end{aligned}$$

Da die Nenner der rationalen Zahlen β'_k und ϱ'_k $(k = 1, \ldots, m)$ vom Index k weitgehend unabhängig sind, überträgt sich das vermöge (15) auf die Nenner $v_\mu(k, l)$ der rationalen Zahlen $s_\mu(k, l)$. Setzen wir in (21) ein, so folgt also wegen

$$\frac{(2k)!}{k!} \leqq (2k)^k, \quad 2^{k(2k+1)} \leqq (2k+1)^{k(k+1)}, \quad \beta'(2k+1) < 2k+1$$

das Ergebnis:

Es existiert eine von μ unabhängige natürliche Zahl $v(k, l)$ mit

$$v_\mu(k, l) \mid v(k, l) \qquad (\mu = 1, \ldots, M(k, l))$$

und

$$v(k, l) < (2k + 1)^{k(l[16k^2 + 40k^2 + 39k + 12] + 8k^2 + 16k + 11)}. \tag{37}$$

6. Wir wollen noch eine grobe Abschätzung für die ganzrationalen Zahlen $b_{\mu\lambda}(k, l)$ angeben. Sie kommen in (15) dadurch herein, daß wir aus den Klammern

$$(\beta'_{\mu_1} x_1 + \cdots + \beta'_{\mu_l} x_l)$$

den Hauptnenner der rationalen Zahlen $\beta'_{\mu\lambda}$ herausziehen. Dieser ist wegen (20) gerade $N_0(m)$ oder ein Teiler davon. Also ist

$$| b_{\mu\lambda}(k, l) | \leqq N_0(m) \max_{\mu=1}^{m} | \beta'_\mu(m) | .$$

Aus (22), (29), (16), (36), (18) folgt als weiteres Ergebnis:

Es ist

$$1 \leqq | b_{\mu\lambda}(k, l) | < (2k + 1)^{4k^2+8k+6} = b(k, l). \tag{38}$$

Im folgenden wollen wir unter

$$v(k, l) \text{ bzw. } b(k, l) \tag{38a}$$

eine beliebige, von μ bzw. μ und λ unabhängige, in k und l bzw. k monotone obere Abschätzung von

$$v_\mu(k, l) \text{ mit } v_\mu(k, l) \mid v(k, l) \text{ bzw. } b_{\mu\lambda}(k, l) \quad \begin{pmatrix} \mu = 1, \ldots, M \\ \lambda = 1, \ldots, l \end{pmatrix}$$

verstehen, insbesondere die in (37) bzw. (38) angegebene.

§ 3. Das Lemma von Kamke [6]).

Lemma 2. *Es seien n, r natürliche Zahlen; dann gibt es dazu ganze Zahlen*

$$\begin{aligned} P &= P(n, r) > 0, \\ A_\nu &= A_\nu(n, r) > 0 && (\nu = 2, \ldots, n + 1), \\ r_\mu &= r_\mu(n, r) > 0 && (\mu = 1, \ldots, P), \\ a_{\mu\lambda} &= a_{\mu\lambda}(n, r) && \begin{pmatrix} \mu = 1, \ldots, P \\ \lambda = 1, \ldots, r \end{pmatrix} \end{aligned}$$

derart, daß folgende n Identitäten in den Veränderlichen $x_1, \ldots, x_r$ gelten:

$$A_\nu(x_1^2 + \cdots + x_r^2)^\nu = \sum_{\mu=1}^{P} r_\mu (a_{\mu 1} x_1 + \cdots + a_{\mu r} x_r)^{2\nu} \qquad (\nu = 2, \ldots, n + 1).$$

Der in [2] gegebene Beweis von Lemma 2 erlaubt es, die Größen von Lemma 2 sofort durch die von Lemma 1 auszudrücken. Die n Identitäten von Lemma 2 entstehen nämlich aus der einen Identität von Lemma 1 für $(n + 1, r + 1)$ dadurch, daß mehrmals nach x_{r+1} differenziert und hernach $x_{r+1} = 0$ gesetzt wird.

Man kann die Beziehungen sofort hinschreiben:

$$P(n, r) = M(n + 1, r + 1);$$

wegen (17) ist also

$$P(n, r) = (2n + 3)^{r+1}. \tag{39}$$

---

[6]) Vgl. [2], S. 90.

Bezeichnen wir mit $C(n, r)$ den Hauptnenner der Zahlen

$$(40) \qquad \frac{b_{\mu\lambda}(n+1, r+1)}{b_{\mu r+1}(n+1, r+1)} \qquad \begin{pmatrix} \mu = 1, \ldots, P \\ \lambda = 1, \ldots, r \end{pmatrix}$$

und mit $T(n, r)$ den Hauptnenner der Zahlen

$$(41) \qquad (2n+2)!\, s_\mu(n+1, r+1) \cdot b_{\mu r+1}(n+1, r+1)^{2(n+1)} \qquad (\mu = 1, \ldots, P),$$

so ist

$$(42) \qquad a_{\mu\lambda}(n, r) = \frac{b_{\mu\lambda}(n+1, r+1)}{b_{\mu r+1}(n+1, r+1)} C(n, r) \qquad \begin{pmatrix} \mu = 1, \ldots, P \\ \lambda = 1, \ldots, r \end{pmatrix}$$

und

$$(43) \qquad r_\mu(n, r) = (2n+2)!\, s_\mu(n+1, r+1) \cdot b_{\mu r+1}(n+1, r+1)^{2(n+1)} \cdot T(n, r) \qquad (\mu = 1, \ldots, P).$$

§ 4. Die Abschätzung von N_1 und N_2.

In den in [4] eingeführten Bezeichnungen ist

$$(44) \qquad N_1 = 4 \sum_{\mu=1}^{P} r_\mu a_{\mu 1}^2$$

und

$$(45) \qquad N_2 = 8 \sum_{\mu=1}^{P} r_\mu a_{\mu 1}^2;$$

dabei sind P, r_μ, $a_{\mu 1}$ Größen, die in Lemma 2 vorkommen. Da in [4] zum Beweis von Satz 1 bzw. Satz 2 das Lemma 2 für $(n, 5)$ bzw. $(n, 9)$ herangezogen wird, ist in (44)

$$(46) \qquad \begin{aligned} P &= P(n, 5), \\ r_\mu &= r_\mu(n, 5), \\ a_{\mu 1} &= a_{\mu 1}(n, 5) \end{aligned}$$

bzw. in (45)

$$(47) \qquad \begin{aligned} P &= P(n, 9), \\ r_\mu &= r_\mu(n, 9), \\ a_{\mu 1} &= a_{\mu 1}(n, 9). \end{aligned}$$

Diese Größen wollen wir jetzt durch die in Lemma 1 vorkommenden Größen ausdrücken und dann die in § 2 gewonnenen Abschätzungen anwenden.

Da in (40), (41) die $b_{\mu\lambda}$ ganze Zahlen und die $s_\mu = \frac{u_\mu}{v_\mu}$ rationale Zahlen sind, ist sicher

$$C(n, r) \leqq \prod_{\pi=1}^{P} b_{\pi r+1}(n+1, r+1)$$

und

$$T(n, r) \leqq v(n+1, r+1) \text{ wegen (37).}$$

Aus (42) folgt unter Beachtung von (38a)

$$(48) \qquad \begin{aligned} a_{\mu\lambda}(n, r) &\leqq b_{\mu\lambda}(n+1, r+1) \cdot \frac{\prod_{\pi=1}^{P} b_{\pi r+1}(n+1, r+1)}{b_{\mu r+1}(n+1, r+1)} \qquad \begin{pmatrix} \mu = 1, \ldots, P \\ \lambda = 1, \ldots, r \end{pmatrix}; \\ &\leqq b(n+1, r+1) \cdot b(n+1, r+1)^{P(n, r)-1} \end{aligned}$$

durch Koeffizientenvergleich in (1) ergibt sich $s_\mu = \frac{u_\mu}{v_\mu} \leqq 1$. Daher folgt unter Berücksichtigung von (38a)

$$s_\mu(n+1, r+1) \cdot T(n, r) \leqq v(n+1, r+1).$$

Also ist in (43)

$$(49) \qquad r_\mu(n, r) \leqq (2n+2)!\, b(n+1, r+1)^{2(n+1)} v(n+1, r+1).$$

Aus (44) bzw. (45) folgen wegen (46) bzw. (47) und wegen (48), (49) die Ungleichungen

$$N_1(n) \leqq 4 \cdot P(n, 5) \cdot (2n+2)!\, b(n+1, 6)^{2(n+1)+2P(n,5)} \cdot v(n+1, 6)$$

bzw.

$$N_2(n) \leqq 8 \cdot P(n, 9) \cdot (2n+2)!\, b(n+1, 10)^{2(n+1)+2P(n,9)} \cdot v(n+1, 10).$$

Daraus folgen wegen (37), (38), (39) schließlich die gewünschten Abschätzungen.

Ergebnis. *Es ist*

$$N_1(n) < (2n+3)^{3(2n+3)^8}$$

und

$$N_2(n) < (2n+3)^{3(2n+3)^{12}}.$$

Diese Schranken lassen sich bei größerer Sorgfalt auf diesem Wege noch beträchtlich verbessern. Unser Ziel war es nur, auf elementarem Wege überhaupt eine explizite Schranke für $N_1(n)$ und $N_2(n)$ anzugeben.

Da meiner Dissertation [5] die gleiche Methode zugrunde liegt wie der vorliegenden Arbeit, sei noch bemerkt, daß sich die in [5] angegebene Schranke

$$g(n) < (2n+1)^{260(n+3)^3 n+8}$$

unter konsequenterer Ausnutzung von Teilbarkeitseigenschaften auf

$$g(n) < (2n+1)^{260(n+1)^8}$$

herabdrücken läßt. Damit tritt also n im obersten Exponenten nicht mehr auf.

Literaturverzeichnis.

[1] *D. Hilbert*, Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem), Math. Ann. **67**, 281—300 (1909).

[2] *E. Kamke*, Verallgemeinerungen des Waring-Hilbertschen Satzes, Math. Ann. **83**, 85—112 (1921).

[3] *E. Kamke*, Über die Zerfällung rationaler Zahlen in rationale Polynomwerte, Math. Z. **12**, 323—328 (1922).

[4] *E. Kamke*, Zum Waringschen Problem für rationale Zahlen und Polynome, Math. Ann. **87**, 238—245 (1922).

[5] *G. J. Rieger*, Zur Hilbertschen Lösung des Waringschen Problems: Abschätzung von $g(n)$. Dissertation Gießen (1953). Auszug: Archiv d. Math. **4**, 275—281 (1953).

[6] *C. L. Siegel*, Darstellung total positiver Zahlen durch Quadrate, Math. Z. **11**, 246—275 (1921), vgl. Satz 2.

[7] *C. L. Siegel*, Generalisation of Waring's problem to algebraic number fields. Amer. J. Math. **66**, 122—136 (1944).

[8] *C. L. Siegel*, Sums of m-th powers of algebraic integers. Ann. Math. **46**, 313—339 (1945).

[9] *E. Stridsberg*, Några elementära undersökninger rörande fakulteter och deras aritmetiska egenskaper. Arkiv för Mat., Astr., Fys. **11**, No. 25 (1916—17).

Gießen (Lahn), Mathem. Institut der Justus-Liebig-Hochschule.

Eingegangen 7. Mai 1954.

Multiplikative Funktionen über euklidischen und Sternverbänden.

Von *Fritz Klein-Barmen* in Wuppertal.

Einleitung.

In der vorliegenden Untersuchung bringe ich einen Satz, der den verbandstheoretischen Kern des in der elementaren Zahlentheorie beheimateten Möbiusschen Umkehrsatzes aufdeckt. Im einzelnen: Zur Erleichterung für den Leser sind in § 1 die zur Lösung des Problems erforderlichen, im wesentlichen bekannten Begriffsbildungen und Sätze aus der Theorie der *quasi-euklidischen*, speziell der *euklidischen* und *Sternverbände* zusammengestellt[1]). In § 2 werden die multiplikativen Verbandsfunktionen eingeführt. Unter Verwendung zweier Funktionaloperatoren und einer der Möbiusschen Funktion nachgebildeten Verbandsfunktion wird in § 3 der eingangs genannte Satz bewiesen.

Zur Vermeidung von Wiederholungen werde folgendes bemerkt. Der jeweils als Operationsbereich fungierende Verband wird mit M bezeichnet. Kleine lateinische Buchstaben — außer m und n — bedeuten Elemente von M; insbesondere sei, wenn M ein unten spitzer Verband ist, e das unterste Element von M. Zur Abkürzung wird

$$x_1 \cup \cdots \cup x_n = \bigcup_{\nu=1}^{n} x_\nu, \quad x_1 \cap \cdots \cap x_n = \bigcap_{\nu=1}^{n} x_\nu$$

gesetzt.

§ 1. Quasi-euklidische, euklidische und Sternverbände.

1. Ist M ein *beliebiger* Verband, so heißt ein Element x genau dann *einfach*, wenn die Unterelemente von x — einschließlich x und, falls M unten spitz ist, auch einschließlich e — einen linearen Teilverband von M bilden.

Ist M ein *unten spitzer* Verband, so heißen zwei nicht notwendigerweise verschiedene Elemente x und y genau dann *fremd* zueinander — in Zeichen: $x \perp y$ — wenn $x \cap y = e$ ist.

2. Es sei M ein *quasi-euklidischer*, d. h. unten spitzer und distributiver Verband.

---

[1]) In systematischer Hinsicht liegen die genannten Verbände zwischen dem distributiven und Booleschen Verband. Realisierungen lassen sich in den verschiedensten Sparten der Mathematik und Logik aufweisen, außer in der Zahlentheorie vornehmlich in Teilgebieten der Algebra und Mengenlehre.

Eng verwandt mit den euklidischen Verbänden sind die *Quaderverbände*; vgl. Skolem [1], S. 12. Die Bezeichnung „Sternverband" geht auf [A. V. II], S. 129 zurück. Vgl. zu § 1 ferner [A. V. III], [A. V. 5] und [Verb. 9], zu dem Satz von der eindeutigen Zerlegbarkeit der Elemente (Satz 3 und 3') auch Birkhoff [13], S. 142. — Bei dieser Gelegenheit möchte ich auf die im Literaturverzeichnis aufgeführte Arbeit von Matsushita aufmerksam machen, worin der Begriff des Verbandes dahingehend verallgemeinert wird, daß für die beiden Elementverknüpfungen das kommutative Gesetz außer Kraft gesetzt wird.

Satz 1. *Mit*

$$x \perp y_\nu \qquad (\nu = 1, \ldots, n)$$

ist

$$x \perp \bigcup_{\nu=1}^{n} y_\nu.$$

Satz 2. *Mit*

$$x \leqq y \cup z, \quad x \perp y$$

ist $x \leqq z$.

Versteht man unter einem EF-System eine endliche oder unendliche Teilmenge N von M derart, daß die Elemente von N verschieden von e, einfach und, falls N aus mindestens zwei Elementen besteht, zu je zweien fremd zueinander sind, so lautet der auf den Sätzen 1 und 2 fußende Hauptsatz über quasi-euklidische Verbände:

Satz 3. *Für jedes von e verschiedene Element x gibt es höchstens ein endliches* EF-*System* $(x_1, \ldots, x_n)$ *derart, daß*

$$x = \bigcup_{\nu=1}^{n} x_\nu \tag{1}$$

ist, wenn von der Reihenfolge der das EF-*System bildenden Elemente abgesehen wird.*

Wir wollen (1) als die *kanonische* Darstellung von x bezeichnen.

Satz 4. *Ein Element x' ist dann und nur dann ein Unterelement des durch* (1) *kanonisch dargestellten Elements x, wenn*

$$x' = \bigcup_{\nu=1}^{n} x'_\nu \qquad (e \leqq x'_\nu \leqq x_\nu) \tag{2}$$

ist.

Offensichtlich erhält man die kanonische Darstellung von x', indem man in (2) die mit e identischen Elemente x'_ν unterdrückt.

Satz 5. *Sind x' und x'' zwei nicht notwendigerweise verschiedene Unterelemente des durch* (1) *kanonisch dargestellten Elements x, so ist*

$$x' \cup x'' = \bigcup_{\nu=1}^{n} (x'_\nu \cup x''_\nu), \quad x' \cap x'' = \bigcup_{\nu=1}^{n} (x'_\nu \cap x''_\nu).$$

Ergänzend werde bemerkt: Ist $e < x < y < z$, so ist mit y auch x kanonisch darstellbar, im allgemeinen aber nicht z.

3. Ein quasi-euklidischer Verband, bei dem jedes von e verschiedene Element eine, also genau eine kanonische Darstellung hat, heißt ein *euklidischer* Verband. Die einfachen Elemente eines euklidischen Verbandes werden auch *Primärelemente*, die EF-Systeme auch *Primärsysteme* genannt.

4. Es sei M ein *Sternverband*, d. h. ein euklidischer Verband, bei dem jedes Primärelement und damit jedes Element nur endlich viele Unterelemente hat. Ein Primärelement x heißt vom *Grad* ξ, wenn x genau $\xi + 1$ Unterelemente hat, wobei x und e mitzuzählen sind. Die Primärelemente ersten Grades heißen *Primelemente*. Ist x ein Primärelement vom Grad ξ mit $\xi \geqq 1$ und ist p das durch $x \geqq p$ eindeutig bestimmte Primelement, so wird

$$x = p^{[\xi]}, \quad p = p^{[1]}, \quad e = p^{[0]}$$

gesetzt. Die Sätze 3, 4 und 5 nehmen die folgende Gestalt an:

Satz 3'. *Für jedes von e verschiedene Element x gibt es genau eine kanonische Darstellung*

$$(1') \qquad x = \bigcup_{\nu=1}^{n} p_\nu^{[\xi_\nu]} \qquad (\xi_\nu \geqq 1).$$

Satz 4'. *Ein Element x' ist dann und nur dann ein Unterelement des durch (1') kanonisch dargestellten Elements x, wenn*

$$(2') \qquad x' = \bigcup_{\nu=1}^{n} p_\nu^{[\xi'_\nu]} \qquad (0 \leqq \xi'_\nu \leqq \xi_\nu)$$

ist.

Satz 5'. *Sind x' und x'' zwei nicht notwendigerweise verschiedene Unterelemente des durch (1') kanonisch dargestellten Elements x, so ist*

$$x' \cup x'' = \bigcup_{\nu=1}^{n} p_\nu^{[\max(\xi'_\nu, \xi''_\nu)]}, \qquad x' \cap x'' = \bigcup_{\nu=1}^{n} p_\nu^{[\min(\xi'_\nu, \xi''_\nu)]}.$$

§ 2. Verbandstheoretische Funktionen.

1. Es sei M ein *beliebiger* Verband und $\varphi(x)$ eine Funktion über M, d. h. eine Funktion, die jedem x eindeutig einen Zahlwert zuordnet. Man bemerkt sofort: Gehören a und b demselben linearen Teilverband von M an, so bestehen für jede Funktion $\varphi(x)$ über M die beiden Identitäten

$$\varphi(a \cup b) + \varphi(a \cap b) = \varphi(a) + \varphi(b),$$
$$\varphi(a \cup b) \cdot \varphi(a \cap b) = \varphi(a) \cdot \varphi(b).$$

2. Es sei M ein *euklidischer* Verband. Eine Funktion $\varphi(x)$ über M heißt genau dann eine *multiplikative Funktion* (Multi-Funktion), wenn für alle a, b mit $a \perp b$

$$(3) \qquad \varphi(a \cup b) = \varphi(a)\, \varphi(b)$$

und außerdem $\varphi(e) \neq 0$, also $\varphi(e) = 1$ ist[2]).

Wie sofort ersichtlich ist, gilt: Mit $\varphi'(x)$ und $\varphi''(x)$ ist auch $\varphi'(x) \cdot \varphi''(x)$ und, falls für alle Argumente $\varphi''(x) \neq 0$ ist, auch $\varphi'(x) : \varphi''(x)$ eine Multi-Funktion.

In Verallgemeinerung von (3) findet statt:

Satz 6. *Ist $\varphi(x)$ eine Multi-Funktion und sind $x_1, \ldots, x_n$ paarweise fremd zueinander, so ist*

$$(4) \qquad \varphi\left(\bigcup_{\nu=1}^{n} x_\nu\right) = \prod_{\nu=1}^{n} \varphi(x_\nu).$$

Beweis klar.

Die Bemerkung in Abschnitt 1 läßt ebenfalls eine Verallgemeinerung zu:

Satz 7. *Ist $\varphi(x)$ eine Multi-Funktion, so ist für alle a, b*

$$(5) \qquad \varphi(a \cup b)\, \varphi(a \cap b) = \varphi(a)\, \varphi(b).$$

Beweis. Es darf $a > e$, $b > e$ angenommen werden. Setzt man $c = a \cup b$ und ist

$$c = \bigcup_{\nu=1}^{n} c_\nu \qquad (\nu = 1, \ldots, n)$$

---

[2]) Auf die analog gebildeten *additiven* Verbandsfunktionen, die durch

$$\varphi(a \cup b) = \varphi(a) + \varphi(b) \qquad (a \perp b)$$

mit $\varphi(e) = 0$ definiert sind, wird in der vorliegenden Arbeit nicht eingegangen.

die kanonische Darstellung von c, so ist nach Satz 4

$$a = \bigcup_{\nu=1}^{n} c'_\nu \qquad (e \leqq c'_\nu \leqq c_\nu),$$

$$b = \bigcup_{\nu=1}^{n} c''_\nu \qquad (e \leqq c''_\nu \leqq c_\nu).$$

Auf Grund der Sätze 5 und 6 ist

$$\varphi(a \cup b)\, \varphi(a \cap b) = \prod_\nu \varphi(c'_\nu \cup c''_\nu) \prod_\nu \varphi(c'_\nu \cap c''_\nu)$$
$$= \prod_\nu \varphi(c'_\nu) \prod_\nu \varphi(c''_\nu),$$

woraus (5) folgt.

Der damit bewiesene Satz liefert das

Kriterium. Eine Funktion $\varphi(x)$ über M ist dann und nur dann eine Multi-Funktion, wenn (5) für alle a, b gilt und $\varphi(e) = 1$ ist.

§ 3. Summator und Reversator. Der Umkehrsatz.

1. In diesem Paragraphen sei M ein *Sternverband* und $\varphi(x)$ eine Multi-Funktion über M. Wegen (4) ist $\varphi(x)$ bekannt, sobald $\varphi(p^{[\xi]})$ für jedes p und jedes von 0 verschiedene ξ bekannt ist. S und R seien zwei Funktionaloperatoren.

2. Die Funktion $S\varphi(x)$ sei durch $S\varphi(e) = 1$ und, wenn

$$x = \bigcup_{\nu=1}^{n} p_\nu^{[\xi_\nu]} \qquad (x > e;\ \nu = 1, \ldots, n)$$

die kanonische Darstellung von x ist, durch

$$S\varphi(x) = \sum_{(\lambda_1, \ldots, \lambda_n)} \varphi\left(\bigcup_{\nu=1}^{n} p_\nu^{[\lambda_\nu]}\right) \tag{6}$$

definiert, wobei über alle die Systeme $(\lambda_1, \ldots, \lambda_n)$ zu summieren ist, für die $0 \leqq \lambda_\nu \leqq \xi_\nu$ ist. $S\varphi(x)$ heißt die *Summatorfunktion* (S-Funktion) von $\varphi(x)$.

Satz 8. *Die S-Funktion einer Multi-Funktion ist ebenfalls eine Multi-Funktion.*

Beweis. Wendet man Satz 6 auf (6) an, so erhält man

$$S\varphi(x) = \sum_{(\lambda_1, \ldots, \lambda_n)} \prod_\nu \varphi(p_\nu^{[\lambda_\nu]}) = \prod_\nu \sum_{\lambda_\nu = 0}^{\xi_\nu} \varphi(p_\nu^{[\lambda_\nu]}) = \prod_\nu S\varphi(p_\nu^{[\xi_\nu]}).$$

3. Ist $\mu(x)$ die durch

$$\mu(p) = -1 \text{ und } \mu(p^{[\xi]}) = 0 \qquad (\xi \geqq 2)$$

festgelegte spezielle Multi-Funktion, so sei $R\varphi(x)$ durch $R\varphi(e) = 1$ und, falls $x > e$ ist, durch

$$R\varphi(x) = \sum_{(\lambda_1, \ldots, \lambda_n)} \mu\left(\bigcup_{\nu=1}^{n} p_\nu^{[\lambda_\nu]}\right) \varphi\left(\bigcup_{\nu=1}^{n} p_\nu^{[\xi_\nu - \lambda_\nu]}\right) \tag{7}$$

definiert, wobei wie soeben über alle die Systeme $(\lambda_1, \ldots, \lambda_n)$ zu summieren ist, für die $0 \leqq \lambda_\nu \leqq \xi_\nu$ ist. $R\varphi(x)$ heißt die *Reversatorfunktion* (R-Funktion) von $\varphi(x)$.

Ähnlich wie Satz 8 beweist man:

Satz 9. *Die R-Funktion einer Multi-Funktion ist ebenfalls eine Multi-Funktion.*

4. Zwischen Summator und Reversator besteht die in dem folgenden Satz beschriebene Wechselbeziehung.

Satz 10 (Umkehrsatz). *Für jede Multi-Funktion $\varphi(x)$ ist*

$$RS\varphi(x) = \varphi(x), \quad SR\varphi(x) = \varphi(x). \tag{8}$$

Beweis. Die Behauptung trifft zu für $x = e$. Sei deshalb $x > e$. Wegen der Sätze 8 und 9 genügt es, anstatt (8) die einfacheren Gleichungen

$$RS\varphi(p^{[\xi]}) = \varphi(p^{[\xi]}), \quad SR\varphi(p^{[\xi]}) = \varphi(p^{[\xi]}) \tag{9}$$

für $\xi \geqq 1$ zu beweisen. Das geschieht so: Setzt man

$$\chi(p^{[\xi]}) = S\varphi(p^{[\xi]}), \tag{10}$$

so ist

$$\chi(p^{[\xi]}) = \sum_{\lambda=0}^{\xi} \varphi(p^{[\lambda]})$$

und weiter

$$\varphi(p^{[\xi]}) = \chi(p^{[\xi]}) - \chi(p^{[\xi-1]}) = \sum_{\lambda=0}^{\xi} \mu(p^{[\lambda]})\, \chi(p^{[\xi-\lambda]}).$$

Also ist

$$\varphi(p^{[\xi]}) = R\chi(p^{[\xi]}). \tag{11}$$

Indem man $\chi(p^{[\xi]})$ zwischen (10) und (11) eliminiert, erhält man die erste der beiden Gleichungen (9). Ähnlich ergibt sich die zweite Gleichung.

Einen in dieselbe Kategorie fallenden Satz, der aber für additive und multiplikative Funktionen in gleicher Weise gilt, habe ich an anderer Stelle bewiesen[3]).

5. Es sei m eine ganze Zahl, die positiv, negativ oder 0 sein kann. S^m und R^m seien die den folgenden Gleichungen genügenden Operatoren[4]):

$$\begin{cases} S^0\varphi(x) = \varphi(x), & R^0\varphi(x) = \varphi(x), \\ S^1 = S, & R^1 = R, \\ S^{m+1} = SS^m, & R^{m+1} = RR^m, \\ S^{-m} = R^{-m}, & R^m = S^{-m}. \end{cases} \tag{12}$$

Nach dem Umkehrsatz hat die beiderseits unendliche Folge

$$\ldots, S^{-1}\varphi(x),\ S^0\varphi(x),\ S^1\varphi(x), \ldots \tag{13}$$

die Eigenschaft, daß jedes ihrer Glieder S-Funktion des linken und R-Funktion des rechten Nachbargliedes ist, während bei der Folge

$$\ldots, R^{-1}\varphi(x),\ R^0\varphi(x),\ R^1\varphi(x), \ldots, \tag{14}$$

die aus (13) durch Umkehrung der Richtung entsteht, Summator und Reversator die Rollen wechseln. Wir wollen (13) bzw. (14) die durch $\varphi(x)$ erzeugte S- bzw. R-Folge und jede Menge von Multi-Funktionen, die gemäß (13) und damit auch gemäß (14) geordnet werden kann, eine Möbiussche *Funktionenklasse* nennen. Man sieht sofort, daß dieselbe durch irgendeine der ihr angehörenden Funktionen vollständig bestimmt ist. Zwei Möbiussche Funktionenklassen sind also entweder identisch oder aber sie haben keine Funktion gemeinsam.

---

[3]) Vgl. [A. V. I] und [A. V. 4].

[4]) Es braucht kaum darauf aufmerksam gemacht zu werden, daß das System (12) noch reduziert werden kann.

6. Wie im vorhergehenden Abschnitt sei m ein Parameter, der alle ganzzahligen Werte annehmen kann. Als *Hauptfunktion* vom Parameter m bezeichnen wir die durch

$$\varphi_m(p^{[\xi]}) = \binom{\xi + m}{\xi} \qquad (\xi \geqq 0)$$

definierte Multi-Funktion $\varphi_m(x)$. Speziell gibt $\varphi_1(x)$ die Anzahl der Unterelemente von x an und ist $\varphi_{-2}(x)$ mit $\mu(x)$ identisch, während

$$\varphi_0(x) = 1 \qquad (x \geqq e),$$
$$\varphi_{-1}(x) = 0 \qquad (x > e)$$

ist.

Satz 11. *Die Menge der Hauptfunktionen über M ist eine Möbiussche Funktionenklasse; dabei ist*

$$S\varphi_m(x) = \varphi_{m+1}(x), \quad R\varphi_m(x) = \varphi_{m-1}(x).$$

Beweis. Wegen der Sätze 8, 9 und 10 reicht es aus, zu zeigen, daß

$$S\varphi_m(p^{[\xi]}) = \varphi_{m+1}(p^{[\xi]}) \qquad (\xi \geqq 0)$$

ist. Das ist aber der Fall, denn für alle ganzzahligen Werte von m ist

$$S\varphi_m(p^{[\xi]}) = \sum_{\lambda=0}^{\xi} \binom{\lambda + m}{\lambda} = \binom{\xi + m + 1}{\xi}.$$

Literaturverzeichnis.

1. *G. Birkhoff*, [13] Lattice theory (2. Aufl. 1948).
2. *F. Klein-Barmen*, [A. V. I] Zur Theorie der abstrakten Verknüpfungen. Math. Ann. **105**, 308—323 (1931).
3. *F. Klein-Barmen*, [A. V. II] Über einen Zerlegungssatz in der Theorie der abstrakten Verknüpfungen. Math. Ann. **106**, 114—130 (1932).
4. *F. Klein-Barmen*, [A. V. III] Über gekoppelte Axiomensysteme in der Theorie der abstrakten Verknüpfungen. Math. Z. **37**, 39—60 (1933).
5. *F. Klein-Barmen*, [Verb. 9] Ein weiterer Beitrag zum Problem der Zerlegung der Elemente gewisser harmonischer Verbände. Deutsche Math. **3**, 46—64 (1938).
6. *F. Klein-Barmen*, [A. V. 4] Über Verbände mit einer weiteren assoziativen und kommutativen Elementverknüpfung. Math. Z. **47**, 85—104 (1940).
7. *F. Klein-Barmen*, [A. V. 5] Molekulare Verbände. Math. Z. **47**, 373—394 (1941).
8. *F. Klein-Barmen*, [N. 3] Pseudoverband und Flechtwerk. Math. Ann. **126**, 138—143 (1953).
9. *S. Matsushita*, [1] Lattices non commutatifs. C. R. Acad. Sci. Paris, 1526—1527 (1953).
10. *Th. Skolem*, [1] Über gewisse „Verbände" oder „lattices". Norske Vid.-Akad., Mat.-Nat. Kl. 7, 1—16 (1936).

Eingegangen 31. Mai 1954.

Zur Zahlentheorie der Quaternionen-Algebren.

Von *Martin Eichler* in Münster.

Einleitung.

Nach H. Brandt[1]) kann man die Klassen von Idealen in einer definiten Quaternionen-Algebra Q der Diskriminante q^2 über dem rationalen Zahlkörper in einem quadratischen Schema $(C_{\mu\nu})$ anordnen, so daß das Folgende gilt: Ist n eine natürliche Zahl und $\pi_{\mu\nu}(n)$ die Anzahl der ganzen Ideale der Norm n in der Klasse $C_{\mu\nu}$, so bestehen zwischen den Matrizen $P(n) = (\pi_{\mu\nu}(n))$ die Relationen:

$$(1) \qquad P(m)\,P(n) = \sum_{t \mid m,n} \chi(t)\, t\, P\left(\frac{mn}{t^2}\right) \quad \text{mit} \quad \chi(t) = \begin{cases} 1 & \text{für } (t, q) = 1, \\ 0 & \text{sonst.} \end{cases}$$

Die $P(n)$ erzeugen demnach einen kommutativen Ring $\mathfrak{M}$. Wir werden hier die Spur von $P(n)$ berechnen, und zwar stellt sie sich als eine Summe über Idealklassenanzahlen imaginär-quadratischer Zahlkörper heraus. Die Bedeutung dieses Ergebnisses ist dreifach.

Erstens kann man die $P(n)$ selber berechnen, sobald man nur ihre Spur, das Schema $(C_{\mu\nu})$ und eine Basis des Ringes $\mathfrak{M}$ kennt (§ 7). Mit Hilfe einer Klassenzahltabelle[2]) kann man also die Matrizen $P(n)$ leicht berechnen und hat damit ein Mittel in der Hand, die Zerlegung einer natürlichen Zahl in Ideale in Q zu studieren, ohne diese Zerlegung explizit durchführen zu müssen. Diese Möglichkeit bedeutet eine befriedigende Abrundung der Idealtheorie in hyperkomplexen Systemen überhaupt, wenn man sich vor Augen hält, daß die Ideale einer zentralen einfachen Algebra über dem rationalen Zahlkörper, die nicht definite Quaternionen-Algebra ist, Hauptideale sind[3]). Für Algebren über algebraischen Zahlkörpern gilt Entsprechendes (s. u.).

Hiermit hängt die Berechnung der Idealklassenzahl von Q, sowie der Typenanzahl maximaler Ordnungen eng zusammen (Satz 11).

Die Kenntnis der $P(n)$ ist besonders deshalb wichtig, weil diese Matrizen eine Darstellung eines Teilringes des Multiplikatorenringes des Körpers der Modulfunktionen der Stufe q liefern. Ja dieser Umstand hat überhaupt erst ihr Studium angeregt. Im Falle $q =$ Primzahl hat E. Hecke 1935 vermutet[4]), daß diese Darstellung treu sei. Wir werden in einer hieran anschließenden Arbeit[5]) Heckes Vermutung bestätigen und sogar wesentlich erweitern. Als Hilfsmittel zu diesem Nachweis wird uns die Spur der $P(n)$ dienen. Das ist die zweite Bedeutung der vorliegenden Arbeit.

---

[1]) *H. Brandt*, Zur Zahlentheorie der Quaternionen, J.-ber. Deutsche Math.-Vereing. **53** (1943), S. 23–57.

[2]) *Hansraj Gupta*, On the class-number of binary quadratic forms, Univ. Nac. Tucumán Revista A **3** (1942), S. 283–299 (bis zur Diskriminante $d = -12500$).

[3]) *M. Eichler*, Über die Idealklassenzahl hyperkomplexer Systeme, Math. Zeitschr. **43** (1938), S. 481–494.

[4]) *E. Hecke*, Analytische Arithmetik der positiven quadratischen Formen, Kgl. Danske Videnskabernes Selskab., Math.-fys. Medd. XVII, 12 (1935), S. 100.

[5]) *M. Eichler*, Über die Darstellung von Modulformen durch Thetareihen, erscheint demnächst in diesem Journal.

Die dritte besteht in der Aufstellung gewisser Klassenzahlrelationen für imaginär-quadratische Zahlkörper (§ 7). Einige von diesen ergeben sich aus den Formeln (1), wenn man die $P(n)$ mittels der Spuren und diese wiederum durch Summen über Klassenzahlen ausdrückt. Alle so erhaltenen Klassenzahlrelationen lassen sich den sogenannten Klassenzahlrelationen der q-ten Stufe unterordnen. Wieviele von ihnen schon früher aufgetreten sind, möchte ich in Anbetracht der schwer übersehbaren Literatur unerörtert lassen.

Der hiermit angedeutete Sachverhalt ist nun aber in vierfacher Hinsicht der Verallgemeinerung fähig. Erstens kann man die Überlegungen für Ideale zu nicht maximalen Ordnungen in Q durchführen. Wegen der genannten Anwendung auf das Darstellungsproblem des Multiplikatorenringes eines Körpers von Modulfunktionen ist diese Verallgemeinerung besonders wichtig. Wir werden uns allerdings auf solche Ideale beschränken, deren Ordnungen eine Diskriminante q^2 mit quadratfreiem q haben; das erlaubt einige Vereinfachungen gegenüber dem allgemeinsten Falle.

Zweitens kann man total definite Quaternionen-Algebren über total reellen Zahlkörpern betrachten. Diese stehen mit den Hilbertschen Modulfunktionen in Zusammenhang. Da ihre Theorie von algebraischer Sicht her aber noch unentwickelt ist, kann man eine Übertragung obigen Satzes über die Darstellung des Multiplikatorenringes höchstens vermuten. Die Klassenzahlrelationen bestehen aber auch jetzt, und zwar sind es Relationen zwischen Relativklassenzahlen total imaginärer quadratischer Erweiterungen eines solchen Körpers.

Drittens kann man den Ganzheitsbegriff abschwächen, indem man Potenzprodukte gewisser Primzahlen als Nenner von im weiteren Sinne ganzen Zahlen zuläßt. Das liefert zwar keine neuen Klassenzahlrelationen; man muß diesen Verallgemeinerungsschritt aber machen, um auch den vierten gleichzeitig mitzuerfassen. Bei diesem wird der Grundkörper ein algebraischer Funktionenkörper mit endlichem Konstantenkörper. Beachtenswerterweise erhält man auch jetzt Klassenzahlrelationen (§ 8), z. B. für die Anzahlen der Divisorenklassen 0-ten Grades in elliptischen oder hyperelliptischen Funktionenkörpern.

Die Allgemeinheit der gestellten Aufgabe macht es erforderlich, manches Bekannte neu zu begründen. Daher wird aus der Literatur nur wenig vorausgesetzt; die Kenntnis des Berichtes von M. Deuring[6]) genügt zum Verständnis, und zwar braucht man ihn nur soweit zu kennen, als er Quaternionen-Algebren betrifft.

Die Arbeit gliedert sich wie folgt: § 1 bringt eine in Hinsicht auf die Allgemeinheit der Aufgabenstellung notwendige Verschärfung des Begriffes einer definiten Quaternionen-Algebra. In § 2 wird die Zahlentheorie „im Kleinen" entwickelt, soweit sie nicht bekannt ist. In § 3 wird die Idealtheorie in der Algebra Q mit der Idealtheorie kommutativer Teilkörper in Beziehung gesetzt; die Schlüsse beruhen hier vorwiegend auf lokalen Überlegungen. § 4 bringt den Begriff des Maßes und das analytische Bestimmungsverfahren für das Maß. § 5 ist der Verallgemeinerung der Matrizen $P(n)$ gewidmet. Die Berechnung der Spur erfolgt in § 6. Nimmt man das Ergebnis voraus, so wird man den § 7 ohne weitere Kenntnis der Arbeit verstehen können; hier werden die wesentlichen bereits oben angedeuteten Schlußfolgerungen gezogen. Beispiele am Schluß sollen die Ergebnisse verdeutlichen. § 8 dient der Durchführung eines Einzelbeispiels in dem Falle, daß der Grundkörper ein Funktionenkörper ist.

---

[6]) *M. Deuring*, Algebren, Ergebn. d. Math. Bd. 4, Heft 1, Berlin 1935.

§ 1. Arithmetisch definite Quaternionen-Algebren.

Der Grundkörper k ist in dieser Arbeit stets entweder ein endlich algebraischer total reeller Zahlkörper oder ein endlich algebraischer Funktionenkörper über einem endlichen Konstantenkörper.

In k werden endlich viele Primdivisoren (d. h. Äquivalente von Klassen von Bewertungen) $\mathfrak{o}_0, \mathfrak{o}_1, \ldots, \mathfrak{o}_r$ als *unendliche Primdivisoren* willkürlich ausgezeichnet, doch sollen im Falle, daß k ein Zahlkörper ist, alle zu den archimedischen Bewertungen gehörigen Primdivisoren unter ihnen vorkommen. Als *ganz* bezeichnen wir alle Elemente $a \in k$, welche höchstens diese $\mathfrak{o}_\varrho$ im Nenner haben, d. h. $|a|_\mathfrak{p} > 1$ gilt höchstens für $\mathfrak{p} = \mathfrak{o}_0, \ldots, \mathfrak{o}_r$. Die ganzen Elemente aus k bilden einen Integritätsbereich $\mathfrak{i}$, die *Hauptordnung* von k. Für die $\mathfrak{i}$-Ideale gilt die bekannte Idealtheorie. Es gilt ferner in folgender Form der

Dirichletsche Einheitensatz. *Die Gruppe der Einheiten von* $\mathfrak{i}$ *ist das direkte Produkt von einer endlichen und* r *unendlichen zyklischen Gruppen.*

Beweis. Für den Fall, daß k ein Funktionenkörper ist, sei auf die Darstellung von H. Hasse[7]) verwiesen. Die dort durchgeführten Überlegungen lassen sich, wenn k ein Zahlkörper ist, leicht mit der gewohnten (engeren) Formulierung des Dirichletschen Satzes kombinieren. Wir werden übrigens unten nur die Existenz einer endlichen Einheitenbasis benutzen.

Ein relativ-quadratischer Zahlkörper K/k oder eine Quaternionen-Algebra Q/k heißt *arithmetisch definit*, wenn alle unendlichen Primdivisoren $\mathfrak{o}_\varrho$ in K teils verzweigt teils träge bzw. in Q verzweigt sind. Sonst heißen K bzw. Q *arithmetisch indefinit*[8]). Aus bekannten Sätzen über relativquadratische Zerfällungskörper einer Quaternionen-Algebra — und diese stimmen bis auf Isomorphie mit den maximalen kommutativen Unterkörpern überein — folgt:

Satz 1. *Die maximalen kommutativen Unterkörper einer arithmetisch definiten Quaternionen-Algebra sind arithmetisch definit.*

Unter einer *Ordnung* $\mathfrak{J}$ einer Quaternionen-Algebra Q versteht man einen Teilring von Q, welcher gleichzeitig ein endlicher $\mathfrak{i}$-Modul ist. Sofern aus dem Zusammenhang nicht ausdrücklich das Gegenteil hervorgeht, verabreden wir, daß eine Ordnung stets 4 linear unabhängige Elemente enthalten soll.

Die Bedeutung der arithmetischen Definitheit beruht in dem folgenden Satz, der, nebenbei bemerkt, für jede arithmetisch indefinite Algebra Q falsch ist:

Satz 2. *Sei* $\mathfrak{J}$ *eine Ordnung (nicht notwendig vom Rang 4) in einer arithmetisch definiten Quaternionen-Algebra* Q, *ferner* $\mathfrak{E}$ *die Gruppe der Einheiten von* $\mathfrak{J}$ *und* $\mathfrak{e}$ *die Gruppe der Einheiten von* $\mathfrak{i}$. *Dann ist der Index* $[\mathfrak{E} : \mathfrak{e}] = e$ *endlich.*

Beweis. Die Normen der Einheiten von $\mathfrak{J}$ bzgl. k bilden eine Untergruppe in $\mathfrak{e}$, welche mindestens alle Quadrate aus $\mathfrak{e}$ enthält; sie hat demnach auf Grund des Dirichletschen Einheitensatzes in $\mathfrak{e}$ einen endlichen Index. Daraus schließt man: Es gibt in $\mathfrak{J}$ endlich viele Einheiten $\varepsilon_1, \ldots, \varepsilon_k$, so daß für jede Einheit ε von $\mathfrak{J}$ ein Index $\varkappa = 1, \ldots, k$ sowie eine Einheit e in $\mathfrak{i}$ existieren mit $n(\varepsilon\varepsilon_\varkappa e) = 1$. Nun braucht man nur noch zu zeigen, daß $\mathfrak{J}$ höchstens endlich viele Einheiten der Norm 1 enthält.

---

[7]) *H. Hasse*, Zahlentheorie, Berlin 1949, S. 436.

[8]) Für den analogen Begriff im Bereiche der quadratischen Formen s. *M. Eichler*, Quadratische Formen und orthogonale Gruppen, Berlin-Göttingen-Heidelberg 1952. — Die Ähnlichkeitsklassen indefiniter Gitter, Math. Zeitschr. **55** (1952), S. 216–252. Die in zahlentheoretischer Hinsicht so einschneidende Grenze verläuft in Wirklichkeit zwischen den arithmetisch definiten und indefiniten Formen (Körpern und Quaternionen-Algebren).

Dazu seien $\iota_1, \ldots, \iota_n$ $(n \leqq 4)$ eine Maximalzahl linear unabhängiger Elemente aus $\mathfrak{J}$ und ε eine Einheit der Norm 1 aus $\mathfrak{J}$. Es ist $\varepsilon = \Sigma\, \iota_\nu p_\nu$, wobei die $p_\nu = p_\nu(\varepsilon)$ einen Hauptnenner haben, der in der Diskriminante der ι_ν aufgeht und infolgedessen beschränkt ist. Gäbe es nun unendlich viele ε dieser Art, so können die $|\, p_\nu(\varepsilon)\,|_{\mathfrak{o}_\varrho}$ nicht sämtlich beschränkt bleiben, da die $p_\nu(\varepsilon)$ aus einem festen $\mathfrak{i}$-Ideal stammen (Beschränktheit des Hauptnenners). Für ein $\mathfrak{o}_\varrho = \mathfrak{o}$ wächst also $|\, p(\varepsilon)\,|_{\mathfrak{o}} = \operatorname{Max}\,(|\, p_1(\varepsilon)\,|_{\mathfrak{o}}, |\, p_2(\varepsilon)\,|_{\mathfrak{o}}, \ldots)$ mit ε über alle Grenzen. Dann sind die Koordinaten der Folge $\tau = p(\varepsilon)^{-1}\varepsilon$ $\mathfrak{o}$-adisch beschränkt, und eine Teilfolge konvergiert gegen einen Grenzwert $\tau_0 \neq 0$. Dabei ist

$$|\, n(\tau_0)\,|_{\mathfrak{o}} = \lim\,(|\, p(\varepsilon)\,|_{\mathfrak{o}})^{-2} n(\varepsilon) = 0, \quad \text{also} \quad n(\tau_0) = 0.$$

Nun liegt aber τ_0 in der $\mathfrak{o}$-adischen Erweiterung von Q, und diese ist wegen der vorausgesetzten arithmetischen Definitheit nullteilerfrei. Daher stellt $\tau_0 \neq 0$, $n(\tau_0) = 0$ einen Widerspruch dar.

§ 2. Ideale quadratfreier Stufe.

Die Diskriminante einer Ordnung einer Quaternionen-Algebra Q ist stets das Quadrat eines $\mathfrak{i}$-Ideals. Das gilt bekanntlich für maximale Ordnungen und überträgt sich von da sofort auf alle anderen Ordnungen. Von Hecke[9]) wurde der Begriff der *Stufe einer definiten quadratischen Form* mit ganzen rationalen Koeffizienten vom größten gemeinsamen Teiler 1 so definiert, daß die zugehörigen Thetareihen Modulformen ebenderselben Stufe sind. In sinngemäßer Übertragung definieren wir hier die *Stufe einer Quaternionen-Ordnung* als

$$\mathfrak{q} = n(\tilde{\mathfrak{J}})^{-1}.$$

Dabei bedeutet $\tilde{\mathfrak{J}}$ das Komplement von $\mathfrak{J}$ und $n(\tilde{\mathfrak{J}})$ den größten gemeinsamen Teiler der Normen der Elemente von $\tilde{\mathfrak{J}}$. Die Stufe ist ein ganzes $\mathfrak{i}$-Ideal. Sie ist das Produkt der Stufen der $\mathfrak{p}$-adischen Erweiterungen von $\mathfrak{J}$.

Satz 3. *Es sei $\mathfrak{J}$ eine Ordnung von quadratfreier Stufe $\mathfrak{q}$ in der Quaternionen-Algebra Q. Für ein in $\mathfrak{q}$ aufgehendes Primideal $\mathfrak{p}$ ist entweder $Q_\mathfrak{p}$ nullteilerfrei und $\mathfrak{J}_\mathfrak{p}$ die (einzige) maximale Ordnung von $Q_\mathfrak{p}$, oder aber $\mathfrak{J}_\mathfrak{p}$ ist isomorph mit der Ordnung der zweireihigen Matrizen mit Elementen aus $\mathfrak{i}_\mathfrak{p}$, wobei das links unten stehende sogar durch $\mathfrak{p}$ teilbar ist.*

Im letzteren Falle werden wir die unmißverständliche Abkürzung

$$\mathfrak{J}_\mathfrak{p} = \begin{pmatrix} \mathfrak{i}_\mathfrak{p} & \mathfrak{i}_\mathfrak{p} \\ \mathfrak{p}_\mathfrak{p} & \mathfrak{i}_\mathfrak{p} \end{pmatrix} \tag{2}$$

benutzen. Die Primteiler der beiden genannten Arten von $\mathfrak{q}$ fassen wir zu den Produkten $\mathfrak{q}_1$ und $\mathfrak{q}_2$ zusammen, die fortan in dieser Bedeutung gebraucht werden. Es gilt also

$$\mathfrak{q} = \mathfrak{q}_1 \mathfrak{q}_2. \tag{3}$$

Beweis. Es sei ι_ν eine $\mathfrak{i}_\mathfrak{p}$-Basis von $\mathfrak{J}_\mathfrak{p}$. Unter der Diskriminantenmatrix verstehen wir die vierreihige Matrix $(s(\bar{\iota}_\mu \iota_\nu)) = (\bar{\iota}_\mu \iota_\nu + \bar{\iota}_\nu \iota_\mu)$, wobei der Querstrich die Konjugiertenbildung bedeutet. Das Komplement $\tilde{\mathfrak{J}} = (\tilde{\iota}_\nu)$ wird durch

$$s(\bar{\iota}_\mu \tilde{\iota}_\nu) = \begin{cases} 1 & \text{für } \mu = \nu, \\ 0 & \text{für } \mu \neq \nu \end{cases}$$

definiert. Es ist $(s(\bar{\tilde{\iota}}_\mu \tilde{\iota}_\nu)) = (s(\bar{\iota}_\mu \iota))^{-1}$, und $n(\tilde{\mathfrak{J}})$ der größten gemeinsamen Teiler aller $\frac{1}{2}\,(s(\bar{\tilde{\iota}}_\mu \tilde{\iota}_\nu) + s(\bar{\tilde{\iota}}_\nu \tilde{\iota}_\mu))$. Damit ist der Anschluß an den Begriff der Stufe für quadratische

[9]) *E. Hecke*, a. a. O.[4]), S. 61.

Formen hergestellt. Dort gilt: Die Diskriminante $|s(\bar{\iota}_\mu \iota_\nu)|$ teilt die 4. Potenz der Stufe, sie teilt sogar schon eine kleinere Potenz der Stufe, falls nicht die Diskriminantenmatrix das $\mathfrak{q}$-fache einer unimodularen Matrix ist, deren Diagonalenglieder sogar durch 2 teilbar sind (falls $\mathfrak{p} \mid 2$)[10]. Da Letzteres nicht der Fall ist, folgt aus der vorausgesetzten Quadratfreiheit der Stufe, daß die Diskriminante das Quadrat der Stufe ist. Dasselbe gilt dann natürlich auch im Großen.

Im Falle, daß $Q_\mathfrak{p}$ nullteilerfrei ist, stellt Satz 3 Bekanntes fest. Es bleibt daher der Nachweis übrig, daß eine

$$\mathfrak{J}_{0\mathfrak{p}} = \begin{pmatrix} \mathfrak{i}_\mathfrak{p} & \mathfrak{i}_\mathfrak{p} \\ \mathfrak{i}_\mathfrak{p} & \mathfrak{i}_\mathfrak{p} \end{pmatrix} \tag{4}$$

umfassende Ordnung $\mathfrak{J}_\mathfrak{p}$ der Diskriminante $\mathfrak{p}^2$ mit (2) isomorph sein muß. Eine Basis von $\mathfrak{J}_{0\mathfrak{p}}$ bilden die Matrixeinheiten δ_{ik}. Eine Basis von $\mathfrak{J}_\mathfrak{p}$ kann man in der Form

$$\begin{aligned} \varepsilon_1 &= a_{11}\delta_{11} + \quad . \quad + b_{21}\delta_{21}, \\ \varepsilon_2 &= \quad a_{22}\delta_{22} + \quad . \quad + c_{21}\delta_{21}, \\ \varepsilon_3 &= \qquad\qquad a_{12}\delta_{12} + d_{21}\delta_{21}, \\ \varepsilon_4 &= \qquad\qquad\qquad a_{21}\delta_{21} \end{aligned}$$

ansetzen, a_{11} usw. $\in \mathfrak{i}_\mathfrak{p}$. Dabei wird $\mathfrak{i}_\mathfrak{p} a_{11} a_{22} a_{12} a_{21} = \mathfrak{p}_\mathfrak{p}$ vorausgesetzt. Die über a_{22}, a_{12}, a_{21} stehenden Koeffizienten darf man jeweils modulo den $\mathfrak{i}_\mathfrak{p}$-Idealen (a_{22}), (a_{12}), (a_{21}) reduziert annehmen, und zwar möglichst zu 0 reduziert. Ist $(a_{11}) = \mathfrak{p}_\mathfrak{p}$, so wären a_{22}, a_{12}, a_{21} Einheiten. $\mathfrak{J}_\mathfrak{p}$ würde dann aber $\delta_{12}\delta_{21} = \delta_{11}$ enthalten, was $(a_{11}) = \mathfrak{p}_\mathfrak{p}$ widerspricht. Aus demselben Grunde ist auch $(a_{22}) \neq \mathfrak{p}_\mathfrak{p}$. Von jetzt ab dürfen wir ohne Beschränkung der Allgemeinheit $a_{11} = a_{22} = 1$ annehmen. Aus Symmetriegründen darf man auch noch $a_{12} = 1$ voraussetzen; a_{21} ist dann ein Primelement. Da $\delta_{11} + \delta_{22} = 1$ in $\mathfrak{J}_\mathfrak{p}$ liegt, muß $b_{21} + c_{21} \equiv 0 \bmod \mathfrak{p}_\mathfrak{p}$ sein, und man kann die Basis so abändern, daß sogar $b_{21} + c_{21} = 0$ ist. Ersetzt man $\mathfrak{J}_\mathfrak{p}$ durch $\begin{pmatrix} 1 & 0 \\ b_{21} & 1 \end{pmatrix}^{-1} \mathfrak{J}_\mathfrak{p} \begin{pmatrix} 1 & 0 \\ b_{21} & 1 \end{pmatrix}$, so gehen b_{21}, c_{21} in 0 über. Da jetzt $\varepsilon_1 \varepsilon_3 = \delta_{12}$ in $\mathfrak{J}_\mathfrak{p}$ liegt, folgt $d_{21} \equiv 0 \bmod \mathfrak{p}_\mathfrak{p}$, und man kann $d_{21} = 0$ machen. Jetzt hat $\mathfrak{J}_\mathfrak{p}$ die behauptete Gestalt (2).

Die Idealtheorie in maximalen Ordnungen wird als bekannt vorausgesetzt. Zu ihrer Übertragung auf nicht maximale Ordnungen genügen einige kurze Andeutungen. Die Ideale entstehen mittels Durchschnittsbildung aus ihren $\mathfrak{p}$-adischen Erweiterungen. Unter einem $\mathfrak{J}_\mathfrak{p}$-Linksideal ist eine Gesamtheit $\mathfrak{M}_\mathfrak{p} = \mathfrak{J}_\mathfrak{p}\mu$ mit einem Nicht-Nullteiler $\mu \in Q_\mathfrak{p}$ zu verstehen. $\mathfrak{M}_\mathfrak{p}$ heißt *ganz*, wenn $\mathfrak{M}_\mathfrak{p} \leqq \mathfrak{J}_\mathfrak{p}$. Die Rechtsordnung von $\mathfrak{M}_\mathfrak{p}$ ist $\mathfrak{J}'_\mathfrak{p} = \mu^{-1}\mathfrak{J}_\mathfrak{p}\mu$. Es ist dann auch $\mathfrak{M}_\mathfrak{p} = \mu\mathfrak{J}'_\mathfrak{p}$, und aus $\mathfrak{M}_\mathfrak{p} \leqq \mathfrak{J}_\mathfrak{p}$ folgt $\mathfrak{M}_\mathfrak{p} \leqq \mathfrak{J}'_\mathfrak{p}$, sowie umgekehrt. Selbstverständlich gilt

Satz 4. *Die Ideale, deren Links- oder Rechtsordnung eine feste quadratfreie Stufe* $\mathfrak{q}$ *haben, bilden ein Gruppoid.*

Bei dem Beweise muß man Satz 3 heranziehen.

Abweichungen vom Gewohnten für die Ordnung (2) sind hauptsächlich bei zwei Fragen zu erwarten. Die erste ist die Abzählung aller ganzen $\mathfrak{J}_\mathfrak{p}$-Linksideale von gegebener Norm. Es bezeichne p ein Primelement in $\mathfrak{i}_\mathfrak{p}$, und

$$\mu = \begin{pmatrix} m_{11} & m_{12} \\ pm_{21} & m_{22} \end{pmatrix}, \qquad \varepsilon = \begin{pmatrix} e_{11} & e_{12} \\ pe_{21} & e_{22} \end{pmatrix}$$

[10]) S. das unter [8]) zitierte Buch des Verf., S. 59/60. Die zweite Hälfte obiger Aussage wird dort zwar nicht ausgesprochen, ist jedoch im Zusammenhang unmittelbar evident.

seien ein beliebiger Nicht-Nullteiler und eine Einheit aus $\mathfrak{J}_\mathfrak{p}$. Wir suchen ε so zu bestimmen, daß

$$\mu' = \varepsilon\mu = \begin{pmatrix} m'_{11} & m'_{12} \\ pm'_{21} & m'_{22} \end{pmatrix} = \begin{pmatrix} e_{11}m_{11} + pe_{12}m_{21} & e_{11}m_{12} + e_{12}m_{22} \\ p(e_{21}m_{11} + e_{22}m_{21}) & pe_{21}m_{12} + e_{22}m_{22} \end{pmatrix}$$

eine Normalgestalt bekommt.

Wenn m_{11} nicht öfter als m_{21} durch $\mathfrak{p}$ teilbar ist, kann man e_{21}, e_{22} so finden, daß $m'_{21} = e_{21}m_{11} + e_{22}m_{21} = 0$ und $(pe_{21}, e_{22}) = \mathfrak{i}_\mathfrak{p}$ ist; pe_{21}, e_{22} kann man als zweite Zeile einer Einheitsmatrix aus $\mathfrak{J}_\mathfrak{p}$ nehmen. Multipliziert man weiter μ' links mit Einheiten der Form $\begin{pmatrix} e_1 & t \\ 0 & e_2 \end{pmatrix}$, wo e_1, e_2 Einheiten von $\mathfrak{i}_\mathfrak{p}$ sind, so kommt man auf die Normalform

$$\begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix}, \quad c \bmod \mathfrak{p}^b \text{ reduziert.} \tag{5a}$$

Ist aber m_{11} durch $\mathfrak{p}$ öfter teilbar als m_{21}, so ist die Gleichung $m'_{11} = e_{11}m_{11} + pe_{12}m_{21} = 0$ mit $(e_{11}, pe_{12}) = \mathfrak{i}_\mathfrak{p}$ lösbar, und für ein solches Paar gibt es ein zweites e_{21}, e_{22} mit $e_{11}e_{22} - pe_{12}e_{21} = 1$. Multipliziert man μ links mit diesem ε und weiter mit Einheiten der Gestalt $\begin{pmatrix} e_1 & 0 \\ pt & e_2 \end{pmatrix}$, so kommt man für μ' auf die Normalform

$$\begin{pmatrix} 0 & p^a \\ p^{b+1} & c \end{pmatrix}, \quad c \bmod \mathfrak{p}^{a+1} \text{ reduziert.} \tag{5b}$$

Die verschiedenen Matrizen (5a), (5b) sind niemals linksseitig assoziiert. Bedeutet $N(\mathfrak{p})$ die Anzahl der Restklassen von $\mathfrak{i} \bmod \mathfrak{p}$, so gibt es

$$1 + 2N(\mathfrak{p}) + \cdots + 2N(\mathfrak{p})^k = 2\frac{N(\mathfrak{p})^{k+1} - 1}{N(\mathfrak{p}) - 1} - 1 \tag{6}$$

ganze $\mathfrak{J}_\mathfrak{p}$-Linksideale der Norm $\mathfrak{p}^k$.

Der zweite Punkt, in dem sich die Idealtheorie der Ordnungen (2) von der der maximalen Ordnungen unterscheidet, ist

Satz 5. *Es sei $\mathfrak{J}_\mathfrak{p}$ die durch (2) definierte Ordnung. Die ambigen $\mathfrak{J}_\mathfrak{p}$-Ideale sind Potenzen von $\mathfrak{P}_\mathfrak{p} = \mathfrak{J}_\mathfrak{p}\pi$. Dabei ist*

$$\pi = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \tag{7}$$

mit einem Primelement p. Es ist $\mathfrak{P}_\mathfrak{p}^2 = \mathfrak{J}_\mathfrak{p}\mathfrak{p}$.

Es gibt also ambige wie nicht ambige ganze $\mathfrak{J}$-Ideale, deren Norm eine Potenz von $\mathfrak{p}$ ist, doch ist auch jetzt ein *ganzes ambiges* $\mathfrak{J}$-Ideal durch seine Norm eindeutig gekennzeichnet.

Beweis. Aus $\pi^{-1}\mathfrak{J}_\mathfrak{p}\pi = \mathfrak{J}_\mathfrak{p}$ folgt, daß $\mathfrak{P}_\mathfrak{p}$ und dessen Potenzen ambig sind. Es sei nun $\mathfrak{J}_\mathfrak{p}\mu$ ein ganzes ambiges Ideal, wobei μ in der Normalgestalt (5a) oder (5b) angenommen wird. Liegt (5b) vor, so ersetze man μ durch $\mu' = \pi\mu$ und erhält ein ebenfalls ambiges Ideal, wobei μ' die Gestalt (5a) hat. Ambige Ideale dieser letzteren Gestalt sind diejenigen, bei denen $a = b$, $c = 0$ ist; Satz 5 behauptet, daß es die einzigen seien. Zum Nachweis transformiere man das allgemeine Element von $\mathfrak{J}_\mathfrak{p}$ mit μ:

$$\begin{pmatrix} p^{-a} & -p^{-a-b}c \\ 0 & p^{-b} \end{pmatrix}\begin{pmatrix} x_{11} & x_{12} \\ px_{21} & x_{22} \end{pmatrix}\begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix} = \begin{pmatrix} x_{11} - p^{1-b}cx_{21} & p^{b-a}x_{12} + p^{-a}c(x_{11} - x_{22}) - p^{1-a-b}c^2x_{21} \\ p^{1+a-b}x_{21} & x_{22} + p^{1-b}cx_{21} \end{pmatrix}.$$

Das transformierte Element ist für alle $x_{ik} \in \mathfrak{i}_\mathfrak{p}$ dann und nur dann wieder in $\mathfrak{J}_\mathfrak{p}$ gelegen, wenn $a = b$ und $c \equiv 0 \bmod \mathfrak{p}^a$ ist, wie behauptet wurde.

§ 3. Kommutative Teilkörper.

Die maximalen kommutativen Teilkörper K einer Quaternionen-Algebra Q/k sind quadratische Erweiterungen von k; ausnahmsweise können sie mit k isomorph sein, und das ist höchstens dann möglich, wenn Q Nullteiler enthält. Einen über k quadratischen Unterkörper von Q wollen wir einen *regulären Unterkörper* nennen.

Die regulären Unterkörper stimmen (bis auf Isomorphie) mit den quadratischen Zerfallungskörpern von Q überein.

Eine Ordnung $\mathfrak{O}$ von K heißt in eine Ordnung $\mathfrak{J}$ von Q *optimal eingebettet*, wenn $\mathfrak{O} = \mathfrak{J} \cap K$ ist[11]). Es gilt der leicht einzusehende

Hilfssatz. *$\mathfrak{O}$ ist in $\mathfrak{J}$ dann und nur dann optimal eingebettet, wenn für alle $\mathfrak{p}$ auch*

$$\mathfrak{O}_\mathfrak{p} = \mathfrak{O}\mathfrak{i}_\mathfrak{p} \tag{8}$$

in $\mathfrak{J}_\mathfrak{p}$ optimal eingebettet ist.

Im allgemeinen ist $\mathfrak{O}$ von der maximalen Ordnung $\mathfrak{O}_0$ von K verschieden. Es sei noch an den Begriff des *Führers* erinnert: Der Führer $\mathfrak{f}$ von $\mathfrak{O}$ ist das umfassendste $\mathfrak{i}$-Ideal in k, für welches $\mathfrak{f}\mathfrak{O}_0 \leqq \mathfrak{O}$ gilt. Im Kleinen besitzen $\mathfrak{O}_0$ und $\mathfrak{O}$ Basen: $\mathfrak{O}_{0\mathfrak{p}} = [1, \omega_0]$, $\mathfrak{O}_\mathfrak{p} = [1, f\omega_0]$, und $\mathfrak{f}_\mathfrak{p} = \mathfrak{i}_\mathfrak{p} f$ ist der $\mathfrak{p}$-adische Beitrag zu $\mathfrak{f}$.

Es gilt nun, die Idealtheorie der Ordnungen $\mathfrak{J}$ von Q mit der Idealtheorie der Ordnungen $\mathfrak{O}$ der regulären Unterkörper K von Q zu verknüpfen. Unter einem $\mathfrak{O}$-Ideal verstehen wir den Durchschnitt von $\mathfrak{O}_\mathfrak{p}$-Idealen $\mathfrak{A}_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}\alpha_\mathfrak{p}$ mit irgendwelchen $\alpha_\mathfrak{p} \neq 0 \in K_\mathfrak{p}$ für alle $\mathfrak{p}$, wobei höchstens endlich viele $\mathfrak{A}_\mathfrak{p} \neq \mathfrak{O}_\mathfrak{p}$ sein sollen (für $\mathfrak{O}_\mathfrak{p}$ vgl. (8)). Bei dieser Fassung des Idealbegriffs bilden die $\mathfrak{O}$-Ideale für eine beliebige Ordnung $\mathfrak{O}$ eine Gruppe, und auch für ihre Einteilung in absolute und relative Idealklassen gilt dasselbe wie für die entsprechenden Begriffe bei maximalen Ordnungen.

Satz 6. *K sei ein regulärer Unterkörper von Q und $\mathfrak{O}$ eine Ordnung in K vom Führer $\mathfrak{f}$. Dann und nur dann gibt es eine Ordnung $\mathfrak{J}$ der Stufe $\mathfrak{q} = \mathfrak{q}_1\mathfrak{q}_2$ in Q, welche in $\mathfrak{O}$ optimal eingebettet ist, wenn folgende beiden Bedingungen erfüllt sind:* 1) $(\mathfrak{f}, \mathfrak{q}_1) = \mathfrak{i}$, 2) *jeder Primteiler $\mathfrak{p}$ von $\mathfrak{q}_2$ geht entweder in $\mathfrak{f}$ auf oder $\mathfrak{p}$ ist in K nicht träge.*

Zur kürzeren Beschreibung des Sachverhalts führen wir ein neues Symbol ein:

$$\left\{\frac{\mathfrak{O}}{\mathfrak{p}}\right\} = \begin{cases} \left(\dfrac{K}{\mathfrak{p}}\right), & \text{falls } \mathfrak{p} \text{ zum Führer von } \mathfrak{O} \text{ prim ist,} \\ 1 & \text{sonst;} \end{cases} \tag{9}$$

dabei bedeutet $\left(\dfrac{K}{\mathfrak{p}}\right)$ das Artinsymbol[12]). Ist speziell die Charakteristik $\neq 2$, so ist das Artinsymbol gleich dem Legendresymbol und für $\mathfrak{O} = \mathfrak{i}[\omega]$:

$$\left\{\frac{\mathfrak{i}[\omega]}{\mathfrak{p}}\right\} = \left\{\frac{s(\omega)^2 - 4n(\omega)}{\mathfrak{p}}\right\} = \begin{cases} \left(\dfrac{s(\omega)^2 - 4n(\omega)}{\mathfrak{p}}\right), & \text{falls } s(\omega)^2 - 4n(\omega) \not\equiv 0 \underline{\text{mod}}\ \mathfrak{p}^2 \\ 1 & \text{falls } s(\omega)^2 - 4n(\omega) \equiv 0 \underline{\text{mod}}\ \mathfrak{p}^2. \end{cases} \tag{9a}$$

---

[11]) *O. F. G. Schilling*, Über gewisse Beziehungen zwischen der Arithmetik hyperkomplexer Zahlsysteme und algebraischer Zahlkörper, Math. Annalen **111** (1935), S. 372–389, bes. S. 376ff.

[12]) Auch im Falle der Charakteristik 2 schreiben wir ihm die Werte -1, 0, 1 zu, je nachdem ob $\mathfrak{p}$ in K träge, verzweigt oder zerlegt ist, im Gegensatz zu *H. Hasse*, Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, Journ. reine angew. Math. **172** (1934), S. 37–54.

Dabei bedeute $t \equiv 0 \underline{\bmod} \mathfrak{p}^2$, daß, unter p ein Primelement verstanden, $tp^{-2} \equiv x^2 \bmod 4\mathfrak{i}$ lösbar ist; für Primteiler $\mathfrak{p}$ von 2 ist das eine schärfere Bedingung als die Kongruenz im gewöhnlichen Sinne. Die Bedingungen von Satz 6 können jetzt so formuliert werden:

$$(10) \qquad \left\{\frac{\mathfrak{O}}{\mathfrak{p}}\right\} \neq 1 \text{ für alle } \mathfrak{p} \mid \mathfrak{q}_1, \quad \left\{\frac{\mathfrak{O}}{\mathfrak{p}}\right\} \neq -1 \text{ für alle } \mathfrak{p} \mid \mathfrak{q}_2 \text{ [13]}.$$

Beweis für Satz 6. Gemäß obigem Hilfssatz müssen die Bedingungen zunächst im Kleinen als notwendig und hinreichend erkannt werden.

Es sei $\mathfrak{p}$ ein Primteiler von $\mathfrak{q}_1$. Dann ist $Q_\mathfrak{p}$ nullteilerfrei und enthält nur eine einzige Ordnung $\mathfrak{J}_\mathfrak{p}$ der Stufe $\mathfrak{p}$; sie ist maximal. Jede Ordnung von $K_\mathfrak{p}$ ist in $\mathfrak{J}_\mathfrak{p}$ enthalten, insbesondere die maximale $\mathfrak{O}_{0\mathfrak{p}}$. Nur diese letztere ist in $\mathfrak{J}_\mathfrak{p}$ optimal eingebettet.

Nun sei $\mathfrak{p}$ ein Primteiler von $\mathfrak{q}_2$. Nach Satz 3 darf man eine Ordnung $\mathfrak{J}_\mathfrak{p}$ der Stufe $\mathfrak{p}$ in der Form (2) ansetzen. $\mathfrak{O}_\mathfrak{p}$ sei in $\mathfrak{J}_\mathfrak{p}$ optimal eingebettet. $\mathfrak{O}_\mathfrak{p}$ besitzt eine $\mathfrak{i}_\mathfrak{p}$-Basis $[1, \omega]$, dabei sei

$$(11) \qquad \omega = \begin{pmatrix} a & b \\ pc & d \end{pmatrix},$$

p wie bisher ein Primelement. Ohne Beschränkung der Allgemeinheit darf $a = 0$ vorausgesetzt werden; denn man könnte nötigenfalls ω durch $\omega - a$ ersetzen. Ist $bc \equiv d \equiv 0 \bmod \mathfrak{p}$, so geht $\mathfrak{p}$ im Führer von $\mathfrak{O}_\mathfrak{p}$ auf. Wenn aber bc oder d zu $\mathfrak{p}$ prim sind, so ist die charakteristische Gleichung $\xi^2 - d\xi - pbc = 0$ von ω entweder in $k_\mathfrak{p}$ lösbar (für $d \not\equiv 0 \bmod \mathfrak{p}$) oder aber $\mathfrak{p}$ ist in $k_\mathfrak{p}(\omega)$ verzweigt ($d \equiv 0 \bmod \mathfrak{p}$). Es ist daher $\left\{\frac{\mathfrak{i}[\omega]}{\mathfrak{p}}\right\} \neq -1$. Ist diese Bedingung aber erfüllt, so kann man ω stets durch eine Matrix (11) mit $a = 0$ und $(b, c, d) = \mathfrak{i}_\mathfrak{p}$ darstellen, und dann ist $\mathfrak{i}_\mathfrak{p}[\omega]$ in $\mathfrak{J}_\mathfrak{p}$ optimal eingebettet.

Ähnlich und völlig elementar verläuft der Nachweis, daß für ein nicht in $\mathfrak{q}_1\mathfrak{q}_2$ aufgehendes $\mathfrak{p}$ jede Ordnung $\mathfrak{O}_\mathfrak{p}$ in die Ordnung (4) optimal eingebettet werden kann.

Es bleibt jetzt noch der Schluß vom Kleinen aufs Große übrig. Wir setzen voraus: Zu jedem $\mathfrak{p}$ gibt es ein $\mathfrak{J}_\mathfrak{p}$ der Stufe $\mathfrak{q}_\mathfrak{p} = \mathfrak{p}$ bzw. $= \mathfrak{i}_\mathfrak{p}$, welches $\mathfrak{O}_\mathfrak{p}$ optimal enthält. Alle in $\mathfrak{q}\mathfrak{f}$ aufgehenden Primideale seien $\mathfrak{p}_\nu$, $\nu = 1, \ldots, n$. Die $\mathfrak{J}_{\mathfrak{p}_\nu}$ sind die $\mathfrak{p}_\nu$-adischen Erweiterungen von gewissen Ordnungen $\mathfrak{J}_\nu$ in Q der Stufe $\mathfrak{q}$. Es sei $\mathfrak{J}_0$ eine maximale Ordnung in Q, welche die Hauptordnung $\mathfrak{O}_0$ von K enthält; es ist also $\mathfrak{O}_0$ in $\mathfrak{J}_0$ optimal eingebettet und daher $\mathfrak{O}_{0\mathfrak{p}}$ in $\mathfrak{J}_{0\mathfrak{p}}$ für alle $\mathfrak{p}$. Nun gibt es eine Ordnung $\mathfrak{J}$ in Q, deren $\mathfrak{p}$-adischen Erweiterungen $\mathfrak{J}_{\mathfrak{p}_\nu} = \mathfrak{J}_{\nu\mathfrak{p}_\nu}$ für $\nu = 1, \ldots, n$ und $\mathfrak{J}_\mathfrak{p} = \mathfrak{J}_{0\mathfrak{p}}$ für alle übrigen $\mathfrak{p}$ sind. Konstruktionsgemäß hat $\mathfrak{J}$ die Stufe $\mathfrak{q}$, und $\mathfrak{O}_\mathfrak{p}$ ist für alle $\mathfrak{p}$ in $\mathfrak{J}_\mathfrak{p}$ optimal eingebettet.

Satz 7. *In zwei Ordnungen $\mathfrak{J}_1, \mathfrak{J}_2$ derselben quadratfreien Stufe sei die Ordnung $\mathfrak{O}$ eines regulären Unterkörpers K von Q optimal eingebettet. Dann gibt es ein $\mathfrak{O}$-Ideal $\mathfrak{A}$ derart, daß $\mathfrak{J}_1\mathfrak{A} = \mathfrak{A}\mathfrak{J}_2$ ist.*

Ist umgekehrt $\mathfrak{O}$ in $\mathfrak{J}_1$ optimal eingebettet, und ist $\mathfrak{A}$ ein $\mathfrak{O}$-Ideal, so ist auch $\mathfrak{O}$ in der Rechtsordnung $\mathfrak{J}_2$ von $\mathfrak{J}_1\mathfrak{A}$ optimal eingebettet.

Beweis [14]). Der zweite Teil des Satzes ergibt sich so: Für ein $\mathfrak{p}$ sei $\mathfrak{A}_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}\alpha$; dann ist $\mathfrak{J}_{1\mathfrak{p}}\mathfrak{A}_\mathfrak{p} = \mathfrak{J}_\mathfrak{p}\alpha$ und $\mathfrak{J}_{2\mathfrak{p}} = \alpha^{-1}\mathfrak{J}_{1\mathfrak{p}}\alpha$. Also $\mathfrak{O}_\mathfrak{p} \leqq \mathfrak{J}_{2\mathfrak{p}}$. Wäre eine größere Ordnung von

[13]) Diese Bedingungen sind zusammen mit $\left(\frac{K}{\mathfrak{o}}\right) \neq 1$ für alle unendlichen Primdivisoren $\mathfrak{o}$ sogar notwendig und hinreichend dafür, daß zu einer abstrakt gegebenen Ordnung $\mathfrak{O}$ ein $\mathfrak{J}$ der Stufe $\mathfrak{q}$ in Q und ein $\mathfrak{O}' \cong \mathfrak{O}$ in $\mathfrak{J}$ existiert.

[14]) Beweise des Satzes für den Fall maximaler Ordnungen $\mathfrak{O}$ und $\mathfrak{J}$, aber beliebiger zentraler einfacher Algebren: 1) *H. Hasse*, Über gewisse Ideale in einer einfachen Algebra, Act. Sci. Ind. **109**, Paris 1934. 2) *E. Noether*, Zerfallende verschränkte Produkte und ihre Maximalordnungen, Act. Sci. Ind. **148**, Paris 1934. 3) *C. Chevalley*, Sur certains idéaux dans un alg bre simple, Abh. Math. Sem. Hamburger Univ. **10** (1934), S. 83–105. 4) *O. F. G. Schilling* a. a. O.[11]).

$K_\mathfrak{p}$ als $\mathfrak{O}_\mathfrak{p}$ in $\mathfrak{J}_{2\mathfrak{p}}$ enthalten, so müßte diese auch in $\mathfrak{J}_{1\mathfrak{p}} = \alpha\mathfrak{J}_{2\mathfrak{p}}\alpha^{-1}$ enthalten sein, im Gegensatz zur Voraussetzung, daß $\mathfrak{O}_\mathfrak{p}$ in $\mathfrak{J}_{1\mathfrak{p}}$ optimal eingebettet sei.

Der erste Teil wird wie der zweite durch Betrachtung an den einzelnen Primstellen bewiesen; dabei werden drei Fälle, je nach dem Schwierigkeitsgrad, unterschieden.

a) $\mathfrak{p} \mid \mathfrak{q}_1$. $Q_\mathfrak{p}$ enthält nur eine einzige Ordnung $\mathfrak{J}_\mathfrak{p}$ der Stufe $\mathfrak{p}$; es ist also $\mathfrak{J}_{1\mathfrak{p}} = \mathfrak{J}_{2\mathfrak{p}}$, und $\mathfrak{A}_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}$ erfüllt das Verlangte.

b) $\mathfrak{p} \nmid \mathfrak{q}_1\mathfrak{q}_2$. Alle Ordnungen der Stufe $\mathfrak{i}_\mathfrak{p}$ sind mit (4) isomorph. Wir setzen $\mathfrak{J}_{1\mathfrak{p}}$ in der Form (4) voraus. Es sei $\mathfrak{J}_{2\mathfrak{p}} = \alpha^{-1}\mathfrak{J}_{1\mathfrak{p}}\alpha$ mit einem $\alpha \in \mathfrak{J}_{1\mathfrak{p}}$. Sind $\varepsilon_1, \varepsilon_2$ zwei Einheiten von $\mathfrak{J}_{1\mathfrak{p}}$, so ist nach Voraussetzung $\mathfrak{O}'_\mathfrak{p} = \varepsilon_2^{-1}\mathfrak{O}_\mathfrak{p}\varepsilon_2$ in $\mathfrak{J}'_{2\mathfrak{p}} = \varepsilon_2^{-1}\mathfrak{J}_{2\mathfrak{p}}\varepsilon_2$ und $\mathfrak{J}_{1\mathfrak{p}} = \varepsilon_2^{-1}\mathfrak{J}_{1\mathfrak{p}}\varepsilon_2$ optimal eingebettet. $\mathfrak{J}'_{2\mathfrak{p}}$ ist die Rechtsordnung von $\mathfrak{J}_{1\mathfrak{p}}\alpha'$, $\alpha' = \varepsilon_1\alpha\varepsilon_2$. Wir ersetzen nun $\mathfrak{O}_\mathfrak{p}, \mathfrak{J}_{2\mathfrak{p}}, \alpha$ durch $\mathfrak{O}'_\mathfrak{p}, \mathfrak{J}'_{2\mathfrak{p}}, \alpha'$, schreiben aber wieder $\mathfrak{O}_\mathfrak{p}, \mathfrak{J}_{2\mathfrak{p}}, \alpha$; und zwar bestimmen wir die Einheiten $\varepsilon_1, \varepsilon_2$ so, daß α die Normalform

$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p^r \end{pmatrix} \tag{12}$$

annimmt (p ein Primelement); wir haben α gleichzeitig möglicherweise durch eine Potenz von p dividiert, was die Allgemeinheit nicht beeinträchtigt. Ist $r = 0$, so ist $\mathfrak{J}_{2\mathfrak{p}} = \mathfrak{J}_{1\mathfrak{p}}$, also nichts zu beweisen; wir nehmen $r > 0$ an. Dann ist

$$\mathfrak{J}_{2\mathfrak{p}} = \begin{pmatrix} \mathfrak{i}_\mathfrak{p} & \mathfrak{p}^r\mathfrak{i}_\mathfrak{p} \\ \mathfrak{p}^{-r}\mathfrak{i}_\mathfrak{p} & \mathfrak{i}_\mathfrak{p} \end{pmatrix}.$$

Sei

$$\mathfrak{O}_\mathfrak{p} = \mathfrak{i}_\mathfrak{p}[\omega], \quad \omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

wo man $a = 0$ voraussetzen kann; denn man könnte ω durch $\omega - a$ ersetzen. Die optimale Einbettbarkeit von $\mathfrak{O}_\mathfrak{p}$ in $\mathfrak{J}_{1\mathfrak{p}}$ und $\mathfrak{J}_{2\mathfrak{p}}$ besagt nun:

$$(b, c, d) = \mathfrak{i}_\mathfrak{p}, \qquad (p^{-r}b, p^r c, d) = \mathfrak{i}_\mathfrak{p}; \tag{13}$$

daraus folgt insbesondere $b \equiv 0 \bmod \mathfrak{p}^r$. Gibt es zwei Elemente $u, v \in \mathfrak{i}_\mathfrak{p}$, für die

$$\mathfrak{J}_{1\mathfrak{p}}\alpha = \mathfrak{J}_{1\mathfrak{p}}(u + v\omega)$$

gilt, so ist $\mathfrak{A}_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}(u + v\omega)$ die $\mathfrak{p}$-Komponente eines Satz 7 genügenden $\mathfrak{O}$-Ideals. Die genannte Gleichung trifft zu, falls

$$(u + v\omega)\,\alpha^{-1} = \begin{pmatrix} u & p^{-r}vb \\ vc & p^{-r}(u + vd) \end{pmatrix} \tag{14}$$

eine Einheit von $\mathfrak{J}_{1\mathfrak{p}}$ ist. Hierzu muß man u, v aus der Kongruenz $u + vd \equiv 0 \bmod \mathfrak{p}$, so bestimmen, daß die Determinante D von (14) eine Einheit wird. Setzt man $v = 1$, $u = -d + p^r u_1$, so ist

$$D = -du_1 + p^r u_1^2 - p^{-r}bc.$$

Ist $d \not\equiv 0 \bmod \mathfrak{p}$, so kann man u_1 immer so finden. Ist aber $d \equiv 0 \bmod \mathfrak{p}$, so muß wegen (13) $p^{-r}bc \not\equiv 0 \bmod \mathfrak{p}$ sein, und $u_1 = 0$ leistet bereits das Verlangte.

c) $\mathfrak{p} \mid \mathfrak{q}_2$. Man nimmt $\mathfrak{J}_{1\mathfrak{p}}$ gemäß Satz 3 in der Form (2) an und $\mathfrak{J}_{2\mathfrak{p}} = \alpha^{-1}\mathfrak{J}_{1\mathfrak{p}}\alpha$, wobei α rechts und links mit Einheiten von $\mathfrak{J}_{1\mathfrak{p}}$ multipliziert werden darf, wie im Schritt b). Das Ziel ist wieder, α in die Gestalt (12) zu bringen; man erreicht es aber nur dann, wenn man α auch noch links und rechts mit Potenzen des Elements (7) multipliziert. Das ist auch erlaubt; denn ersetzt man $\mathfrak{O}_\mathfrak{p}, \alpha, \mathfrak{J}_{2\mathfrak{p}}$ durch $\mathfrak{O}'_\mathfrak{p} = \pi^{-r_2}\mathfrak{O}_\mathfrak{p}\pi^{r_2}$, $\alpha' = \pi^{r_1}\alpha\pi^{r_2}$, $\mathfrak{J}'_{2\mathfrak{p}} = \pi^{-r_2}\mathfrak{J}_{2\mathfrak{p}}\pi^{r_2}$, so ist $\mathfrak{O}'_\mathfrak{p}$ in $\mathfrak{J}_{1\mathfrak{p}} = \pi^{-r_1}\mathfrak{J}_{1\mathfrak{p}}\pi^{r_1}$ (nach Satz 5) und in $\mathfrak{J}'_{2\mathfrak{p}} = \alpha'^{-1}\mathfrak{J}_{1\mathfrak{p}}\alpha' = \pi^{-r_2}\alpha^{-1}\pi^{-r_1}\mathfrak{J}_{1\mathfrak{p}}\pi^{r_1}\alpha\pi^{r_2}$ (ebenfalls nach Satz 5) optimal eingebettet.

Durch linksseitige Multiplikation von α mit einer Einheit ε_1 stellt man zunächst eine der Normalformen (5a, b) her, wobei im Falle (5b) linksseitige Multiplikation mit π auf (5a) führt. Einen gemeinsamen Teiler aller Koeffizienten von (5a) darf man herausheben und daher $(p^a, p^b, c) = \mathfrak{i}_\mathfrak{p}$ voraussetzen. Ist nun $b = 0$, so kann man auch $c = 0$ machen, und die Transformation mit π vertauscht p^a und p^b, so daß jetzt α in die Gestalt (12) übergeführt ist. Im Falle $a = 0$ wird diese Gestalt durch rechtsseitige Multiplikation mit der Einheit $\begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix}$ hergestellt. Ist aber $a > 0$, $b > 0$, so ist $c \not\equiv 0 \bmod \mathfrak{p}$. Dann bilde man zunächst

$$\alpha' = \alpha\pi^{-1} = \begin{pmatrix} p^a & c \\ 0 & p^b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}^{-1} = \begin{pmatrix} c & p^{a-1} \\ p^b & 0 \end{pmatrix};$$

bringt man α' durch linksseitige Multiplikation mit einer Einheit und eventuell mit π auf die Gestalt (5a), so fällt wegen $c \not\equiv 0 \bmod \mathfrak{p}$ nunmehr $a = 0$ aus, und man kann wie oben weiter schließen.

Wie im Schritt b) nimmt man hierauf

$$\mathfrak{O}_\mathfrak{p} = \mathfrak{i}_\mathfrak{p}[\omega], \quad \omega = \begin{pmatrix} 0 & b \\ pc & d \end{pmatrix}$$

an, wobei wieder

$$(b, c, d) = \mathfrak{i}_\mathfrak{p}, \qquad (p^{-r}b, p^r c, d) = \mathfrak{i}_\mathfrak{p}$$

sein muß. Es sind $u, v \in \mathfrak{i}_\mathfrak{p}$ so aufzufinden, daß

$$(u + v\omega)\,\alpha^{-1} = \begin{pmatrix} u & p^{-r}vb \\ pvc & p^{-r}(u + vd) \end{pmatrix}$$

eine Einheit in $\mathfrak{J}_{1\mathfrak{p}}$ ist. Ist $d \not\equiv 0$ mod. $\mathfrak{p}$, so leistet dieses $v = 1$, $u = -d + p^r$. Ist aber $d \equiv 0$ mod. $\mathfrak{p}$, so wird der Ansatz unter b) folgendermaßen abgeändert: Es ist

$$(-d + \omega)\,(\pi\alpha)^{-1} = \begin{pmatrix} p^{-r}b & p^{-1}d \\ 0 & c \end{pmatrix}$$

eine Einheit in $\mathfrak{J}_{1\mathfrak{p}}$, also $\mathfrak{J}_{1\mathfrak{p}}(-d + \omega) = \mathfrak{J}_{1\mathfrak{p}}\pi\alpha$, d. h. $\mathfrak{A}_\mathfrak{p} = \mathfrak{O}_\mathfrak{p}(-d + \omega)$ leistet das Verlangte.

§ 4. Klassenzahl und Maß.

Von jetzt ab machen wir die Voraussetzung, daß die Quaternionen-Algebra Q/k arithmetisch definit sei. Die Anzahl H der Linksidealklassen, in die die Linksideale für eine Ordnung $\mathfrak{J}$ der Stufe $\mathfrak{q}$ in Q zerfallen, ist dann i. a. > 1. (Sie ist von $\mathfrak{J}$ unabhängig und gleichzeitig gleich der Anzahl der Rechtsidealklassen für ein $\mathfrak{J}$.) Sei $\mathfrak{J}_1 = \mathfrak{M}_1, \ldots, \mathfrak{M}_H$ ein Repräsentantensystem der Linksidealklassen für $\mathfrak{J} = \mathfrak{J}_1$. Die Rechtsordnungen $\mathfrak{J}_\nu$ der $\mathfrak{M}_\nu$ repräsentieren dann alle Typen von Ordnungen dieser Stufe; die Anzahl der Typen heiße T.

Wir denken uns die $\mathfrak{M}_\nu$ so numeriert, daß $\mathfrak{J}_1, \ldots, \mathfrak{J}_T$ zu verschiedenen Typen gehören, und für jedes ν sei $\mathfrak{T}_{\nu\mu}$ $(\mu = 1, \ldots, H_\nu)$ ein Repräsentantensystem aller Klassen ambiger $\mathfrak{J}_\nu$-Ideale. Dann ist $\mathfrak{M}_\nu\mathfrak{T}_{\nu\mu}$ $(\mu = 1, \ldots, H_\nu;\ \nu = 1, \ldots, T)$ auch ein Repräsentantensystem aller $\mathfrak{J}$-Linksklassen und demnach

$$H = \sum_{\nu=1}^{T} H_\nu. \tag{15}$$

Die Klassenzahlen H_ν der ambigen $\mathfrak{J}_\nu$-Ideale stehen mit den Automorphismenanzahlen der $\mathfrak{J}_\nu$ in Beziehung. Auf Grund von Satz 5 und seines Analogons für maximale Ordnungen läßt sich jedes ambige $\mathfrak{J}_\nu$-Ideal $\mathfrak{T}_\nu$ als Produkt eines ganzen ambigen $\mathfrak{J}_\nu$-Ideals $\mathfrak{T}_{\nu 0}$, dessen Norm in $\mathfrak{q}$ aufgeht, und eines $\mathfrak{i}$-Ideals $\mathfrak{t}$ in k schreiben: $\mathfrak{T}_\nu = \mathfrak{T}_{\nu 0}\mathfrak{t}$. Mit einem Repräsentantensystem $\mathfrak{a}_\gamma$ $(\gamma = 1, \ldots, h_0)$ der Idealklassen in k gilt dann also für jedes ambige $\mathfrak{J}_\nu$-Ideal die Darstellung $\mathfrak{T}_\nu = \mathfrak{T}_{\nu 0}\mathfrak{a}_\gamma t$, $t \in k$. Andererseits kann man $\mathfrak{T}_\nu = \mathfrak{T}_{\nu\mu}\alpha$ mit einem Repräsentanten $\mathfrak{T}_{\nu\mu}$ der H_ν ambigen $\mathfrak{J}_\nu$-Klassen und einem ambigen Hauptideal $\mathfrak{J}_\nu\alpha$ schreiben. Es ist $\alpha^{-1}\mathfrak{J}_\nu\alpha = \mathfrak{J}_\nu$, d. h. α induziert einen inneren Automorphismus von $\mathfrak{J}_\nu$. Werden durch α_ϱ $(\varrho = 1, \ldots, q_\nu)$ alle inneren Automorphismen induziert (q_ν wird sich nebenbei als endlich herausstellen), so ist $\alpha = \alpha_\varrho t$, $t \in k$. Durch $\mathfrak{T}_\nu = \mathfrak{T}_{\nu\mu}\alpha$ ist α aber nur bis auf eine Einheit ε als linksseitigen Faktor gegeben, und ε läßt sich in der Weise $\varepsilon = \varepsilon_\sigma e$ mit einem maximalen System ε_σ $(\sigma = 1, \ldots, e_\nu)$ bzgl. $\mathfrak{i}$ nicht assoziierten Einheiten von $\mathfrak{J}_\nu$ und einer Einheit e von $\mathfrak{i}$ schreiben. Das bedeutet, durch $\mathfrak{T}_\nu$ ist α genau e_ν-deutig festgelegt. Vergleich beider Darstellungen von $\mathfrak{T}_\nu$ ergibt die Formel $h_0 2^\varkappa = \dfrac{H_\nu q_\nu}{e_\nu}$ oder

$$\frac{H_\nu}{e_\nu} = h_0 \frac{2^\varkappa}{q_\nu}. \tag{16}$$

Dabei bedeuten: H_ν die Anzahl der Klassen ambiger $\mathfrak{J}$-Ideale, q_ν die Anzahl der inneren Automorphismen von $\mathfrak{J}_\nu$, e_ν den Index der Einheitengruppe von $\mathfrak{i}$ in der Einheitengruppe $\mathfrak{E}_\nu$ von $\mathfrak{J}_\nu$, h_0 die Idealklassenzahl von $\mathfrak{i}$, $\varkappa$ die Anzahl der Primteiler von $\mathfrak{q}$.

Die Klassenzahl H und die Typenzahl T werden unten als ein Nebenergebnis unserer Untersuchungen erscheinen. Zu ihrer Berechnung brauchen wir aber das sogenannte *Maß*, die Summe

$$M = \sum_{\nu=1}^{T} \frac{H_\nu}{e_\nu}, \tag{17}$$

welches mit den gewohnten transzendenten Hilfsmitteln berechnet wird, falls k ein algebraischer Zahlkörper und $\mathfrak{i}$ die Ordnung der im gewöhnlichen Sinne ganzen Zahlen aus k ist. Für Funktionenkörper k als Grundkörper ist die Maßbestimmung bisher nicht durchgeführt worden.

Der $\mathfrak{p}$-Beitrag für ein $\mathfrak{p} \mid \mathfrak{q}_2$ zu der Zetafunktion $\zeta(s)$ einer Ordnung der Stufe $\mathfrak{q} = \mathfrak{q}_1\mathfrak{q}_2$ ist nach § 2 (Formel (6))

$$\zeta_\mathfrak{p}(s) = \sum_{i=0}^{\infty}\left(2\frac{N(\mathfrak{p})^{i+1}-1}{N(\mathfrak{p})-1} - 1\right) N(\mathfrak{p})^{-2is} = \frac{1 + N(\mathfrak{p})^{1-2s}}{(1 - N(\mathfrak{p})^{-2s})(1 - N(\mathfrak{p})^{1-2s})}.$$

Die Zetafunktion selber ist deshalb

$$\zeta(s) = \zeta_0(2s)\,\zeta_0(2s-1) \prod_{\mathfrak{p} \mid \mathfrak{q}_1} (1 - N(\mathfrak{p})^{1-2s}) \prod_{\mathfrak{p} \mid \mathfrak{q}_2} (1 + N(\mathfrak{p})^{1-2s})$$

Trägt man dieser Abweichung von dem für maximale Ordnungen Bekannten Rechnung, so ergibt sich[15])

$$M = \frac{2h_0\zeta_0(2)D_0^{3/2}}{(2\pi)^{2n}} \prod_{\mathfrak{p} \mid \mathfrak{q}_1} (N(\mathfrak{p}) - 1) \prod_{\mathfrak{p} \mid \mathfrak{q}_2} (N(\mathfrak{p}) + 1). \tag{18}$$

Dabei bedeuten: n den Grad, h_0 die Idealklassenzahl, $\zeta_0(s)$ die Zetafunktion, D_0 die Diskriminante von k.

[15]) *M. Eichler*, Über die Idealklassenzahl total definiter Quaternionen-Algebren, Math. Zeitschr. 43 (1937), S. 102–109.

§ 5. Die Anzahlmatrizen.

Wie in § 4 sei $\mathfrak{M}_\nu (\nu = 1, \ldots, H)$ ein Vertretersystem der $\mathfrak{J}_1$-Linksidealklassen. Dann ist $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu (\nu = 1, \ldots)$ ein Vertretersystem aller $\mathfrak{J}_\mu$-Linksidealklassen.

Wir bilden nun mit H. Brandt[16]) die *Anzahlmatrizen*

$$P(\mathfrak{n}) = (\pi_{\mu\nu}(\mathfrak{n})), \tag{19}$$

wo $\pi_{\mu\nu}(\mathfrak{n})$ die Anzahl der ganzen $\mathfrak{J}_\mu$-Linksideale der Norm $\mathfrak{n}$ ist, welche mit $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu$ linksäquivalent sind.

Einer durch $\mathfrak{n}$ vertretenen i-Idealklasse wird folgendermaßen eine gewisse Permutation $\lambda(\nu)$ der Ziffern $1, \ldots, H$ zugeordnet: $\mathfrak{M}_\nu\mathfrak{n}$ ist mit $\mathfrak{M}_{\lambda(\nu)}$ linksäquivalent. $L(\mathfrak{n})$ sei diejenige Matrix, welche an der Stelle $\mu\nu$ den Koeffizienten 1 hat, wenn $\nu = \lambda(\mu)$ ist, sonst 0. Dann gilt ersichtlich

$$L(\mathfrak{m}\cdot\mathfrak{n}) = L(\mathfrak{m})\, L(\mathfrak{n}). \tag{20}$$

Neben den $P(\mathfrak{n})$ und $L(\mathfrak{n})$ brauchen wir noch die Diagonalmatrix E, bestehend aus den in § 4 erklärten Einheitenindizes $e_\nu = [\mathfrak{E}_\nu : \mathfrak{e}]$ für die Rechtsordnungen $\mathfrak{J}_\nu$ der $\mathfrak{M}_\nu$. Da die Rechtsordnungen von $\mathfrak{M}_\nu\mathfrak{n}$ und $\mathfrak{M}_\nu$ übereinstimmen, permutiert $\lambda(\nu)$ nur Indizes, für welche e_ν gleich ist. Also gilt

$$L(\mathfrak{n})\, E = E L(\mathfrak{n}). \tag{21}$$

Wir beweisen jetzt die wichtige Symmetrieformel

$$P(\mathfrak{n})\, E = (P(\mathfrak{n})\, L(\mathfrak{n})\, E)^{\cdot} = E L(\mathfrak{n})^{-1} \dot{P}(\mathfrak{n}). \tag{22}$$

Der Punkt bedeutet Spiegelung der Matrix. Die ganzen $\mathfrak{J}_\mu$-Linksideale der Norm $\mathfrak{n}$ aus der Linksklasse von $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu$ seien $\mathfrak{A}_\varrho = \mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu\alpha_\varrho$ $(\varrho = 1, \ldots, \pi_{\mu\nu}(\mathfrak{n}))$. Man ordnet ihnen folgendermaßen ganze $\mathfrak{J}_\nu$-Linksideale derselben Norm aus der Linksklasse von $\mathfrak{M}_\nu^{-1}\mathfrak{M}_\mu\mathfrak{n}$ zu:

$$\mathfrak{A}_\varrho \to \mathfrak{A}_\varrho^* = \overline{\alpha_\varrho \mathfrak{A}_\varrho \alpha_\varrho^{-1}} = \overline{\mathfrak{M}}_\nu \overline{\mathfrak{M}}_\mu^{-1} \overline{\alpha}_\varrho = \frac{n(\mathfrak{M}_\nu)}{n(\mathfrak{M}_\mu)}\, \mathfrak{M}_\nu^{-1}\mathfrak{M}_\mu \overline{\alpha}_\varrho. \tag{23}$$

Diese Zuordnung ist i. a. nicht eindeutig, denn α_ϱ ist durch $\mathfrak{A}_\varrho$ nur bis auf eine Einheit ε_ν von $\mathfrak{J}_\nu$ als linksseitigen Faktor bestimmt. Die Zuordnung (23) ist umkehrbar, wobei man beachten muß, daß auch jetzt $\overline{\alpha}_\varrho$ durch $\mathfrak{A}_\varrho^*$ nur bis auf eine Einheit $\overline{\varepsilon}_\mu$ aus $\mathfrak{J}_\mu$ als linksseitigen Faktor bestimmt ist. Läßt man nun ε_ν, ε_μ je ein Repräsentantensystem von $\mathfrak{e}$ in den Einheitengruppen $\mathfrak{E}_\nu$, $\mathfrak{E}_\mu$ durchlaufen, so repräsentieren $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu\varepsilon_\nu\alpha_\varrho\varepsilon_\mu$ die $\mathfrak{A}_\varrho$ genau e_ν-fach und $\overline{\mathfrak{M}}_\nu\overline{\mathfrak{M}}_\mu^{-1}\overline{\varepsilon}_\mu\overline{\alpha}_\varrho\overline{\varepsilon}_\nu$ die $\mathfrak{A}_\varrho^*$ genau e_μ-fach, während die Zuordnung (23) jetzt umkehrbar eindeutig wird. Daher hat man

$$\pi_{\mu\nu}(\mathfrak{n})\, e_\nu = \pi_{\nu\lambda(\mu)}(\mathfrak{n})\, e_\mu$$

oder in Matrixschreibweise die Gleichung (22).

Für die Anzahlmatrizen gelten die folgenden Multiplikationsgesetze:

$$P(\mathfrak{m})\, P(\mathfrak{n}) = P(\mathfrak{m}\cdot\mathfrak{n}), \text{ falls } (\mathfrak{m}, \mathfrak{n}) = \mathfrak{i} \tag{24}$$

$$P(\mathfrak{p}^a)\, P(\mathfrak{p}^b) = \sum_{\nu=0}^{b} N(\mathfrak{p})^\nu P(\mathfrak{p}^{a+b-2\nu})\, L(\mathfrak{p}^{-1})^\nu, \qquad a \geqq b, \tag{25}$$

falls $\mathfrak{p}$ ein nicht in $\mathfrak{q}$ aufgehendes Primideal ist. Für einen Primteiler $\mathfrak{p}$ von $\mathfrak{q}_1$ gilt

$$P(\mathfrak{p}^a)\, P(\mathfrak{p}^b) = P(\mathfrak{p}^{a+b}). \tag{26}$$

[16]) A. a. O.[1]). Brandt nennt sie *Heckesche Matrizen*, nicht mit vollem Recht, denn sie wurden von ihm selber eingeführt, allerdings in der Absicht, gewisse funktionentheoretische Ergebnisse Heckes arithmetisch zu deuten. Den Übertragungen der Anzahlmatrizen auf quadratische Formen beliebiger (vorwiegend gerader) Variablenzahl ist das IV. Kapitel meines unter [8]) zitierten Buches gewidmet.

Die Gleichung (24) bringt bekanntlich zum Ausdruck, daß die Dirichletreihe mit Matrixkoeffizienten

$$\sum_{\mathfrak{n}} \frac{P(\mathfrak{n})}{N(\mathfrak{n})^s}$$

eine Eulersche Produktentwicklung besitzt. (25) und (26) besagen, daß die Faktoren in diesem Produkt im Sinne Heckes kanonisch sind. Für die Primteiler $\mathfrak{p}$ von $\mathfrak{q}_2$ gilt dieses aber nicht mehr[17]).

Beweis von (24). Ein ganzes $\mathfrak{J}_\mu$-Linksideal $\mathfrak{C}$ der Norm $\mathfrak{m}\mathfrak{n}$ erlaubt eine und nur eine Produktzerlegung $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$ in ganze Ideale $\mathfrak{A}$, $\mathfrak{B}$ der Normen $\mathfrak{m}, \mathfrak{n}$, wenn $(\mathfrak{m}, \mathfrak{n}) = \mathfrak{i}$ ist. $\mathfrak{C}$ durchlaufe die ganzen $\mathfrak{J}_\mu$-Linksideale der Norm $\mathfrak{m}\mathfrak{n}$ aus der Klasse von $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu$; dabei möge $\mathfrak{A}$ der Klasse von $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\varrho$ angehören: $\mathfrak{A} = \mathfrak{M}_\mu^{-1}\mathfrak{M}_\varrho\alpha$. Dann ist $\mathfrak{B} = \alpha^{-1}\mathfrak{M}_\varrho^{-1}\mathfrak{M}_\nu\beta = \alpha^{-1}\mathfrak{B}'\alpha$, und $\mathfrak{B}'$ ist gleichzeitig mit $\mathfrak{B}$ ganz. Die Zuordnung $\mathfrak{B} \longleftrightarrow \mathfrak{B}'$ ist bei gegebenem α eineindeutig. Multipliziert man umgekehrt alle ganzen $\mathfrak{A}$ der Norm $\mathfrak{m}$ dieser Art mit allen ganzen $\mathfrak{B}$ der Norm $\mathfrak{n}$, so bekommt man ganze $\mathfrak{C}$ der Norm $\mathfrak{m}\mathfrak{n}$ aus der Klasse von $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu$. Folglich gilt

$$\pi_{\mu\nu}(\mathfrak{m}\mathfrak{n}) = \sum_{\varrho} \pi_{\mu\varrho}(\mathfrak{m})\, \pi_{\varrho\nu}(\mathfrak{n}), \tag{27}$$

wie behauptet wurde.

Beweis von (26). $\mathfrak{p}$ sei ein Primteiler von $\mathfrak{q}_1$. Es gibt dann für jedes $a > 0$ genau ein ganzes Ideal der Norm $\mathfrak{p}^a$ und von vorgeschriebener Linksordnung; es ist ambig. Die Gleichung (27) ist jetzt auch gültig für $\mathfrak{m} = \mathfrak{p}^a$, $\mathfrak{n} = \mathfrak{p}^b$ in dem Sinne, daß die $\pi_{\mu\nu}(\mathfrak{p}^a)$ jeweils 0 oder 1 sind, und zwar gibt es zu einem μ genau ein ν, so daß $\pi_{\mu\nu}(\mathfrak{p}^a) = 1$ ist, sowie umgekehrt.

Beweis von (25). Wir behandeln zunächst den Spezialfall $b = 1$. $\mathfrak{p}$ sei ein zu $\mathfrak{q}$ teilerfremdes Primideal. Ein ganzes Ideal $\mathfrak{C}$ heiße primitiv, wenn $\mathfrak{p}^{-1}\mathfrak{C}$ nicht mehr ganz ist, sonst imprimitiv. Ein ganzes primitives $\mathfrak{J}_\mu$-Linksideal $\mathfrak{C}$ der Norm $\mathfrak{p}^{a+1}$ erlaubt eine und nur eine Produktzerlegung $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$ in ganze Ideale $\mathfrak{A}$ der Norm $\mathfrak{m} = \mathfrak{p}^a$ und $\mathfrak{B}$ der Norm $\mathfrak{n} = \mathfrak{p}$. Ein ganzes imprimitives $\mathfrak{C}$ dieser Norm erlaubt dagegen soviele solche Zerlegungen, als es Ideale $\mathfrak{B}$ der Norm $\mathfrak{p}$ überhaupt gibt, d. h. $N(\mathfrak{p}) + 1$; denn es ist $\overline{\mathfrak{B}}\mathfrak{B} = \mathfrak{p}\mathfrak{J}$, wo $\mathfrak{J}$ die Rechtsordnung von $\mathfrak{B}$ bezeichnet. Die übrigen zu (24) führenden Überlegungen bleiben gültig, und es gilt jetzt

$$P(\mathfrak{p}^a)\, P(\mathfrak{p}) = P_p(\mathfrak{p}^{a+1}) + (N(\mathfrak{p}) + 1)\, P_i(\mathfrak{p}^{a+1}), \tag{28}$$

wenn P_p, P_i die P entsprechenden Anzahlmatrizen der primitiven und imprimitiven Ideale sind. Ersichtlich ist $P = P_p + P_i$. Ferner sind die imprimitiven Ideale $\mathfrak{C} = \mathfrak{C}'\mathfrak{p}$ mit ganzem $\mathfrak{C}'$, und wenn $\mathfrak{C}$ der Linksklasse von $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu$ angehört, so gehört $\mathfrak{C}'$ der Linksklasse von $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu\mathfrak{p}^{-1}$ an. Das ergibt $P_i(\mathfrak{p}^{a+1}) = P(\mathfrak{p}^{a-1})\, L(\mathfrak{p}^{-1})$. Demnach ist (28) mit (25) im Falle $b = 1$ identisch.

Die Überlegungen bleiben wörtlich richtig, wenn man $n(\mathfrak{A}) = \mathfrak{p}$, $n(\mathfrak{B}) = \mathfrak{p}^a$ verlangt. Dann vertauschen sich in (25) die Faktoren auf der linken Seite. Da das Ergebnis sich nicht ändert, sind hiernach $P(\mathfrak{p}^a)$ und $P(\mathfrak{p})$ vertauschbar. Multipliziert man $P(\mathfrak{p})^2 = P(\mathfrak{p}^2) + N(\mathfrak{p})\, L(\mathfrak{p}^{-1})$ links oder rechts mit $P(\mathfrak{p})$, so erhält man

$$P(\mathfrak{p})^3 = P(\mathfrak{p})\, P(\mathfrak{p}^2) + N(\mathfrak{p})\, P(\mathfrak{p})\, L(\mathfrak{p}^{-1}) = P(\mathfrak{p}^2)\, P(\mathfrak{p}) + N(\mathfrak{p})\, L(\mathfrak{p}^{-1})\, P(\mathfrak{p}).$$

Wegen der Vertauschbarkeit von $P(\mathfrak{p})$ und $P(\mathfrak{p}^2)$ ist also $P(\mathfrak{p})$ mit $L(\mathfrak{p}^{-1})$ vertauschbar. Daraus folgt weiter: $P(\mathfrak{p}^a)$ und $L(\mathfrak{p}^{-1})$ sind vertauschbar.

---

[17]) Zur Möglichkeit nicht kanonischer Eulerprodukte s. *Hecke* a. a. O. [4]), S. 49.

Allgemein wird (25) durch vollständige Induktion bezüglich b unter der Voraussetzung $a \geqq b$ bewiesen. Multiplikation von (25) mit $P(\mathfrak{p})$ ergibt wegen der soeben festgestellten Vertauschbarkeitsregeln:

$$P(\mathfrak{p}^a)\,(P(\mathfrak{p}^{b+1}) + N(\mathfrak{p})\,L(\mathfrak{p}^{-1})P(\mathfrak{p}^{b-1}))$$
$$= \sum_{\nu=0}^{b} (N(\mathfrak{p})^\nu\, L(\mathfrak{p}^{-1})^\nu\, P(\mathfrak{p}^{a+b+1-2\nu}) + N(\mathfrak{p})^{\nu+1}\, L(\mathfrak{p}^{-1})^{\nu+1}\, L(\mathfrak{p}^{a+b+1-2(\nu+1)})).$$

Benutzt man (25) noch einmal für $b - 1$ statt b, so läßt sich dies umformen zu

$$P(\mathfrak{p}^a)\,P(\mathfrak{p}^{b+1}) = \sum_{\nu=0}^{b} (N(\mathfrak{p})^\nu\, L(\mathfrak{p}^{-1})^\nu\, P(\mathfrak{p}^{a+b+1-2\nu}) + N(\mathfrak{p})^{\nu+1}\, L(\mathfrak{p}^{-1})^{\nu+1}\, P(\mathfrak{p}^{a+b+1-2(\nu+1)}))$$
$$- \sum_{\nu=0}^{b-1} N(\mathfrak{p})^{\nu+1}\, L(\mathfrak{p}^{-1})^{\nu+1}\, P(\mathfrak{p}^{a+b+1-2(\nu+1)})$$
$$= \sum_{\nu=0}^{b+1} N(\mathfrak{p})^\nu\, L(\mathfrak{p}^{-1})^\nu\, P(\mathfrak{p}^{a+b+1-2\nu}),$$

was zu beweisen war.

Satz 8. *Jeder kommutative durch Anzahlmatrizen $P(\mathfrak{n})$ sowie Matrizen $L(\mathfrak{n})$ erzeugte Ring $\mathfrak{M}$ über dem Körper der reellen Zahlen ist halbeinfach; ein solcher Ring ist z. B. der durch alle $L(\mathfrak{n})$ und alle $P(\mathfrak{n})$ mit $(\mathfrak{n}, \mathfrak{q}_2) = \mathfrak{i}$ erzeugte.*

Der nicht ganz einfache Beweis zerfällt in vier Schritte a)—d), von denen bereits c) ausreichend ist, wenn die Idealklassenzahl für $\mathfrak{i}$ gleich 1 ist.

a) Der durch alle $L(\mathfrak{n})$ über dem Körper K der reellen Zahlen erzeugte Ring $\mathfrak{L}$ ist kommutativ und halbeinfach, denn die $L(\mathfrak{n})$ bilden eine Darstellung der Klassengruppe in $\mathfrak{i}$. Daher ist $\mathfrak{L}$ die direkte Summe von Körpern $\mathfrak{L}_\nu$, die teils mit K, teils mit $K(i)$ isomorph sind. Es sei

$$L(\mathfrak{n}) = \sum_{\nu=1}^{m} L_\nu(\mathfrak{n}) \tag{29}$$

die Zerlegung in die direkten Summanden $L_\nu(\mathfrak{n}) \in \mathfrak{L}_\nu$. Der Spiegelungsautomorphismus

$$L(\mathfrak{n}) \longleftrightarrow \dot{L}(\mathfrak{n}) = L(\mathfrak{n})^{-1} \tag{30}$$

induziert in den $\mathfrak{L}_\nu$ teilweise Automorphismen, teils vertauscht er verschiedene $\mathfrak{L}_\nu$ paarweise. Bei passender Numerierung gilt

$$\dot{\mathfrak{L}}_\nu = \mathfrak{L}_\nu\ (\nu = 1, \ldots, n),\quad \dot{\mathfrak{L}}_{n+\nu} = \mathfrak{L}_{n+r+\nu}\ (\nu = 1, \ldots, r;\ n + 2r = m).$$

Wegen (29), (30) muß dann

$$\dot{L}_\nu(\mathfrak{n}) = L_\nu(\mathfrak{n})^{-1}\ (\nu = 1, \ldots, n),\quad \dot{L}_{n+\nu}(\mathfrak{n}) = L_{n+r+\nu}(\mathfrak{n})^{-1}\ (\nu = 1, \ldots, r) \tag{31}$$

gelten.

Für ein ν bilden die $L_\nu(\mathfrak{n})$ eine reelle Darstellung 1. oder 2. Grades der Idealklassengruppe von $\mathfrak{i}$; eine Darstellung 2. Grades ist stets mit einer ebenen Drehungsgruppe äquivalent. Es gibt daher entweder in $\mathfrak{L}_\nu$ oder wenigstens in $\mathfrak{L}_\nu(i)$ eine Matrix $\Lambda_\nu(\mathfrak{n})$, welche der Gleichung

$$\Lambda_\nu(\mathfrak{n})^2 \doteq L_\nu(\mathfrak{n}) \tag{32}$$

genügt; und zwar ist die Adjunktion von i dann und nur dann erforderlich, wenn die Darstellung vom 1. Grade und $L_\nu(\mathfrak{n}) = -1$ war. Wir dehnen im letzteren Falle die Definition des Spiegelungsautomorphismus auf $\mathfrak{L}(i)$ durch die Festsetzung aus, daß $\dot{i} = \bar{i} = -i$ sei. Geschieht das für alle ν, so wird dadurch der Spiegelungsautomorphismus auch für $\mathfrak{L}(i)$ erklärt, und zwar so, daß $L \longleftrightarrow \dot{L}$ Spiegelung und Übergang zum konjugiert Komplexen bedeutet.

Mit dieser Festsetzung gelten wegen (31), (32) die n ersten Gleichungen in

(33) $\dot{\Lambda}_\nu(\mathfrak{n}) = \Lambda_\nu(\mathfrak{n})^{-1} (\nu = 1, \ldots, n)$, $\Lambda_{n+\nu}(\mathfrak{n}) = \Lambda_{n+r+\nu}(\mathfrak{n})^{-1} (\nu = 1, \ldots, r)$;

die r letzteren lassen sich dadurch sicherstellen, daß die noch unbestimmten Vorzeichen der $\Lambda_\nu(\mathfrak{n})$ geeignet fixiert werden. Aus (32), (33) folgt nun

(34) $$\Lambda(\mathfrak{n})^2 = L(\mathfrak{n}), \quad \dot{\Lambda}(\mathfrak{n}) = \Lambda(\mathfrak{n})^{-1} \text{ für } \Lambda(\mathfrak{n}) = \sum_{\nu=1}^{m} \Lambda_\nu(\mathfrak{n}).$$

b) Im zweiten Schritt zeigen wir, daß die $L(\mathfrak{n})$ mit allen $P(\mathfrak{m})$ vertauschbar sind. Man nehme ein zu $\mathfrak{m}\mathfrak{q}$ primes Primideal $\mathfrak{p}$ aus der Klasse von $\mathfrak{n}$; dann gilt $L(\mathfrak{p}) = L(\mathfrak{n})$. Unter Benutzung von (20) bis (24) rechnet man nun

$$P(\mathfrak{m}\mathfrak{p})\, E = E\; L(\mathfrak{m}\mathfrak{n})^{-1} \dot{P}(\mathfrak{m}\mathfrak{p}) = E\; L(\mathfrak{m})^{-1} L(\mathfrak{n})^{-1} \dot{P}(\mathfrak{m})\, \dot{P}(\mathfrak{p})$$
$$= P(\mathfrak{m})\, P(\mathfrak{p})\, E = P(\mathfrak{m})\, E\; L(\mathfrak{n})^{-1} \dot{P}(\mathfrak{p}) = E\; L(\mathfrak{m})^{-1} \dot{P}(\mathfrak{m})\, L(\mathfrak{n})^{-1} P(\mathfrak{p}),$$

also

(35) $$U \dot{P}(\mathfrak{p}) = \left(L(\mathfrak{n})^{-1} \dot{P}(\mathfrak{m}) - P(\mathfrak{m})\, L(\mathfrak{n})^{-1}\right) \dot{P}(\mathfrak{p}) = 0.$$

Ebenso folgt

(36) $$\left(L(\mathfrak{n})^{-2} \dot{P}(\mathfrak{m}) - \dot{P}(\mathfrak{m})\, L(\mathfrak{n})^{-2}\right) \dot{P}(\mathfrak{p}^2) = \left(L(\mathfrak{n})^{-1} U + U L(\mathfrak{n})^{-1}\right) \dot{P}(\mathfrak{p}^2) = 0.$$

Multipliziert man (35) rechts mit $\dot{P}(\mathfrak{p})$, so entsteht wegen (25)

(37) $$U\left(\dot{P}(\mathfrak{p}^2) - N(\mathfrak{p})\, L(\mathfrak{p})\right) = 0.$$

Nun war oben im Beweis von (25) festgestellt worden, daß $P(\mathfrak{p})$, $P(\mathfrak{p}^2)$ und $L(\mathfrak{n}) = L(\mathfrak{p})$ vertauschbar sind; $\dot{P}(\mathfrak{p})$ und $\dot{P}(\mathfrak{m})$ sind wegen (24) vertauschbar. Daher sind die Faktoren in (35) und mithin die in (37) vertauschbar, und hieraus folgt die Vertauschbarkeit von U und $\dot{P}(\mathfrak{m})$. Das ergibt $UL(\mathfrak{p}) = L(\mathfrak{p})\, U$ oder

(38) $$L(\mathfrak{n})^{-1} U - U L(\mathfrak{n})^{-1} = 0.$$

Setzt man in (36) $\dot{P}(\mathfrak{p}^2) = \dot{P}(\mathfrak{p})^2 - N(\mathfrak{p})\, L(\mathfrak{p})$ ein, so folgt

$$\left(L(\mathfrak{n})^{-1} U + U L(\mathfrak{n})^{-1}\right) \left(\dot{P}(\mathfrak{p})^2 - N(\mathfrak{p})\, L(\mathfrak{p})\right) = 0.$$

Wegen der Vertauschbarkeit von $\dot{P}(\mathfrak{p})$ und $L(\mathfrak{n})$ und wegen (35) folgt daraus weiter

$$L(\mathfrak{n})^{-1} U + U L(\mathfrak{n})^{-1} = 0$$

und in Verbindung mit (38)

(39) $$U = L(\mathfrak{n})^{-1} \dot{P}(\mathfrak{m}) - \dot{P}(\mathfrak{m})\, L(\mathfrak{n})^{-1} = L(\mathfrak{n})\, P(\mathfrak{m}) - P(\mathfrak{m})\, L(\mathfrak{n}) = 0.$$

c) Man bilde die Diagonalmatrix W mit den Elementen $|\sqrt{e_\nu}|$. Für sie gilt

(40) $$W^2 = E, \quad W L(\mathfrak{n}) = L(\mathfrak{n})\, W;$$

das Letztere ergibt sich im gleichen Zuge wie (21). Mit W und der Matrix (34) setze man für jedes $\mathfrak{n}$

(41) $$R(\mathfrak{n}) = \Lambda(\mathfrak{n})\, W^{-1} P(\mathfrak{n})\, W.$$

Dann folgt einerseits aus (22) und (34), andererseits aus den festgestellten Vertauschbarkeitsregeln und (40)

(42) $$\dot{R}(\mathfrak{n}) = R(\mathfrak{n}).$$

Ferner folgt aus (24) bis (26) unter den dort gemachten Voraussetzungen

$$R(\mathfrak{m})\,R(\mathfrak{n}) = R(\mathfrak{m}\mathfrak{n}) \qquad \text{für } (\mathfrak{m}, \mathfrak{n}) = \mathfrak{i} \tag{43}$$

$$R(\mathfrak{p}^a)\,R(\mathfrak{p}^b) = \sum_{\nu=0}^{b} N(\mathfrak{p})^\nu\, R(\mathfrak{p}^{a+b-2\nu}) \qquad \text{für } a \geqq b, \tag{44}$$

$$R(\mathfrak{p}^a)\,R(\mathfrak{p}^b) = R(\mathfrak{p}^{a+b}). \tag{45}$$

Wegen (43) bis (45) erzeugen die $R(\mathfrak{n})$ mit $(\mathfrak{n}, \mathfrak{q}_2) = \mathfrak{i}$ einen kommutativen Ring. $\mathfrak{R}$ sei ein aus irgendwelchen $R(\mathfrak{n})$ erzeugter kommutativer Ring. Die Erzeugenden von $\mathfrak{R}$ sind wegen (42) symmetrische reelle bzw. hermitesche Matrizen. Sie lassen sich bekanntlich gleichzeitig durch eine reelle orthogonale bzw. unitäre Matrix auf Hauptachsen transformieren. Daher ist $\mathfrak{R}$ halbeinfach.

d) Der Ring $\mathfrak{M}$ entstehe durch Komposition der Ringe $\mathfrak{R}$ und $\mathfrak{L}$. Nach a) ist $\mathfrak{L}$ halbeinfach und nach b) mit $\mathfrak{R}$ elementweise vertauschbar. Der Durchschnitt $\mathfrak{N} = \mathfrak{R} \cap \mathfrak{L}$ ist halbeinfach und die direkte Summe von Körpern $\mathfrak{N}_\nu$. Die direkte Zerlegung $\mathfrak{N} = \Sigma\mathfrak{N}_\nu$ induziert natürlich direkte Zerlegungen $\mathfrak{R} = \Sigma\mathfrak{R}_\nu$, $\mathfrak{L} = \Sigma\mathfrak{L}_\nu$, und das Kompositum von $\mathfrak{R}$ und $\mathfrak{L}$ ist die direkte Summe der direkten Produkte $\mathfrak{R}_\nu \times \mathfrak{L}_\nu$ mit den $\mathfrak{N}_\nu$ als Grundkörpern. Das direkte Produkt halbeinfacher hyperkomplexer Systeme über einem Körper der Charakteristik 0 ist wieder halbeinfach. Daraus folgt die Halbeinfachheit von $\mathfrak{M}$.

Die Summe der Koeffizienten von $P(\mathfrak{n})$ in der ν-ten Zeile ist gleich der Anzahl der ganzen $\mathfrak{J}_\nu$-Linksideale der Norm $\mathfrak{n}$, also von ν unabhängig.

Satz 9. *Die Zeilensummen $p(\mathfrak{n})$ der Anzahlmatrizen $P(\mathfrak{n})$ sind für alle Zeilen gleich, und zwar gilt*

$$p(\mathfrak{m})\,p(\mathfrak{n}) = p(\mathfrak{m}\mathfrak{n}) \qquad \textit{für } (\mathfrak{m}, \mathfrak{n}) = \mathfrak{i}, \tag{46}$$

$$p(\mathfrak{p}^a) = \frac{N(\mathfrak{p})^{a+1} - 1}{N(\mathfrak{p}) - 1} \qquad \textit{für } \mathfrak{p} \nmid \mathfrak{q}, \tag{47}$$

$$p(\mathfrak{p}^a) = 1 \qquad \textit{für } \mathfrak{p} \mid \mathfrak{q}_1, \tag{48}$$

$$p(\mathfrak{p}^a) = 2\,\frac{N(\mathfrak{p})^{a+1} - 1}{N(\mathfrak{p}) - 1} \qquad \textit{für } \mathfrak{p} \mid \mathfrak{q}_2. \tag{49}$$

Für die letztere Anzahl vgl. (6).

§ 6. Die Spur der Anzahlmatrizen.

Zum Verständnis des Folgenden vergegenwärtige man sich die Bedeutung der Bezeichnungen in § 4 sowie des Symbols (9). Mit $\mathfrak{o}_\nu$ bezeichnen wir wie in § 1 die unendlichen Primdivisoren. $\left(\frac{s, n}{\mathfrak{o}_\nu}\right)$ sei das Artinsymbol $\left(\frac{K \mid k}{\mathfrak{o}_\nu}\right)$ für den durch Auflösung der quadratischen Gleichung

$$\xi^2 - s\xi + n = 0$$

über k entstehenden Körper; es möge die Werte 1 (Zerlegtheit), 0 (Verzweigtheit), -1 (Trägheit) annehmen[12]).

Auf Grund des Dirichletschen Einheitensatzes (§ 1) gibt es endlich viele Einheiten e_ϱ ($\varrho = 1, \ldots, R$) von $\mathfrak{i}$ derart, daß jede Einheit e in der Form $e = e'^2 e_\varrho$ mit einer weiteren Einheit e' und einem geeigneten ϱ geschrieben werden kann. Ein solches minimales Vertretersystem der „Quadratklassen" der Einheiten in $\mathfrak{i}$ wird im folgenden festgehalten.

Satz 10. *Die Spur der Anzahlmatrix $P(\mathfrak{n})$ ist 0, wenn $\mathfrak{n}$ kein Hauptideal ist.*

Es sei $\mathfrak{n} = \mathfrak{i}n_0$. Dann bilde man erstens alle Produkte $n = n_0 e_\varrho$ mit den soeben erklärten Einheiten e_ϱ, zweitens alle $s \in \mathfrak{i}$ derart, daß für alle unendlichen Primdivisoren $\mathfrak{o}_\nu$ die Artinsymbole $\left(\frac{s, n}{\mathfrak{o}_\nu}\right) \neq 1$ und $s^2 \neq 4n$ sind[18]*, drittens alle Ordnungen*

$$\mathfrak{O} \geqq \mathfrak{i}[\xi], \quad \xi^2 - s\xi + n = 0. \tag{50}$$

Bezeichnen nun $h(\mathfrak{O})$ und $w(\mathfrak{O})$ die Anzahl der Idealklassen von $\mathfrak{O}$ und den Index der Einheitengruppe von $\mathfrak{i}$ in der von $\mathfrak{O}$, so ist die Spur

$$Sp(P(\mathfrak{n})) = (M) + \frac{1}{2} \sum_{\varrho, s, \mathfrak{O}} \prod_{\mathfrak{p} \mid \mathfrak{q}_1} \left(1 - \left\{\frac{\mathfrak{O}}{\mathfrak{p}}\right\}\right) \prod_{\mathfrak{p} \mid \mathfrak{q}_2} \left(1 + \left\{\frac{\mathfrak{O}}{\mathfrak{p}}\right\}\right) \frac{h(\mathfrak{O})}{w(\mathfrak{O})}, \tag{51}$$

wo (M) gleich dem Maß (17) oder 0 ist, je nachdem ob $\mathfrak{n}$ das Quadrat eines Hauptideals ist oder nicht.

Beweis. Ist $\mathfrak{n}$ kein Hauptideal, so gibt es auch kein Hauptideal $\mathfrak{J}_\nu \alpha$ der Norm $\mathfrak{n}$, also sind alle $\pi_{\nu\nu}(\mathfrak{n}) = 0$, und die Spur ist 0. Von jetzt ab werde

$$\mathfrak{n} = \mathfrak{i}n_0$$

vorausgesetzt.

Es seien $\mathfrak{J}_\nu \alpha_\lambda (\lambda = 1, \ldots, \pi_{\nu\nu}(\mathfrak{n}))$ alle $\mathfrak{J}_\nu$-Linkshauptideale der Norm $\mathfrak{n}$ und ε_σ $(\sigma = 1, \ldots, e_\nu)$ ein Repräsentantensystem aller Nebengruppen von $\mathfrak{e}$ in der Einheitengruppe $\mathfrak{E}_\nu$ von $\mathfrak{J}_\nu$. Dann ist $\alpha^0_{\sigma\lambda} = \varepsilon_\sigma \alpha_\lambda$ ein maximales System bzgl. $\mathfrak{e}$ nicht assoziierter $\alpha \in \mathfrak{J}_\nu$ mit $\mathfrak{i}n(\alpha) = \mathfrak{n}$. Diese $\alpha^0_{\sigma\lambda}$ kann man noch jeweils mit einer Einheit $e \in \mathfrak{e}$ so multiplizieren, daß die Produkte $\alpha_{\sigma\lambda} = e\alpha^0_{\sigma\lambda}$ die Normen $n(\alpha) = n_0 e_\varrho = n$ haben. Ist umgekehrt $n(\alpha) = n = n_0 e_\varrho$, $\alpha \in \mathfrak{J}_\nu$, so ist $\alpha = e\alpha_{\sigma\lambda}$ mit einem Indexpaar $\sigma\lambda$ und einer Einheit $e \in \mathfrak{e}$. Normenbildung ergibt $n_0 e_\varrho = e^2 n_0 e_{\varrho'}$, und da die e_ϱ ein Repräsentantensystem der Quadratklassen in $\mathfrak{e}$ bilden sollten, muß $e^2 = 1$, also $e = \pm 1$ sein. Es folgt hieraus: Bezeichnet $c_\nu(n)$ die Anzahl der $\alpha \in \mathfrak{J}_\nu$ der Norm n, so gilt

$$\pi_{\nu\nu}(\mathfrak{n}) = \frac{1}{2e_\nu} \sum_\varrho c_\nu(n_0 e_\varrho). \tag{52}$$

Die $\alpha \in \mathfrak{J}_\nu$ werden nun zuerst nach ihrer Norm, sodann nach ihrer Spur

$$n(\alpha) = n = n_0 e_\varrho, \quad s(\alpha) = s \tag{53}$$

und endlich nach der Ordnung

$$\mathfrak{O}_\nu = \mathfrak{J}_\nu \cap k(\alpha) \tag{54}$$

angeordnet, welche in $\mathfrak{J}_\nu$ optimal eingebettet ist. Diese Ordnung ist also mit einer der Ordnungen (50) isomorph.

Vorweg ist der Grenzfall $\alpha \in k$ zu studieren, der dann und nur dann auftreten kann, wenn $\mathfrak{n} = \mathfrak{i}a^2$ ist. Dann kommen $+a$ und $-a$ in der Anzahl $c_\nu(n_0 e_\varrho)$ vor, und der Beitrag der Ideale $\mathfrak{J}_\nu a$ zu (52) ist $\frac{1}{e_\nu}$, zu der Spur wegen (17) also M, wie behauptet wurde. Von jetzt ab sei α nicht in k gelegen, also $s^2 \neq 4n$.

Man bilde alle Ordnungen (50) und suche alle zu $\mathfrak{O}$ isomorphen in $\mathfrak{J}_\nu$ optimal eingebetteten Ordnungen $\mathfrak{O}_\nu$ auf. Ist $g_\nu(\mathfrak{O})$ deren Anzahl, so gilt

$$c_\nu(n) = 2 \sum_{s, \mathfrak{O}} g_\nu(\mathfrak{O}). \tag{55}$$

---

[18]) Man könnte zeigen, daß es nur endlich viele solche s gibt. Aber auch ohne diesen Nachweis erkennt man die Summe (51) als endlich, denn Summenwert wie Summanden sind Anzahlen, d. h. natürliche Zahlen $\geqq 0$.

Zu jedem $\alpha \in \mathfrak{J}_\nu$ mit Spur und Norm (53) gehört nämlich genau eine Ordnung (54), umgekehrt wird α durch Spur und Norm in einer Ordnung $\mathfrak{O}_\nu$ zweideutig (d. h. bis auf Konjugiertenbildung eindeutig) festgelegt.

Aus (52), (55) und (16) folgt nun

$$(56) \qquad Sp(P(\mathfrak{n})) = (M) + \sum_{\nu=1}^{T} \sum_{\mathfrak{O}} \frac{H_\nu g_\nu(\mathfrak{O})}{e_\nu} = (M) + h_0 \sum_{\mathfrak{O}} \sum_{\nu=1}^{T} 2^\varkappa \frac{g_\nu(\mathfrak{O})}{q_\nu},$$

wobei die Summation über den Index ϱ, sowie s in der über $\mathfrak{O}$ enthalten sein soll. Die Beschränkung auf solche s, für die $\left(\frac{s, n}{\mathfrak{o}_\nu}\right) \neq 1$ für alle $\mathfrak{o}_\nu$ ist, braucht hier nicht besonders erwähnt zu werden, da für die übrigen s von selbst $g_\nu(\mathfrak{O}) = 0$ wäre. Der Beweis besteht nun in der Ausführung der Summe über ν, wobei $\mathfrak{O}$ jeweils festgehalten wird[19]). Der Kürze halber schreiben wir im folgenden g_ν statt $g_\nu(\mathfrak{O})$.

Ohne Beschränkung der Allgemeinheit darf $g_1 \neq 0$ vorausgesetzt werden. Die sämtlichen in den $\mathfrak{J}_\nu$ optimal eingebetteten und zu $\mathfrak{O}$ isomorphen Ordnungen seien $\mathfrak{O}_1 = \mathfrak{O}_{11}, \ldots, \mathfrak{O}_{1g_1}, \ldots, \mathfrak{O}_{\nu\mu}, \ldots$ ($\nu = 1, \ldots, T$; $\mu = 1, \ldots, g_\nu$). Es gibt dann Elemente $\gamma_{\nu\mu} \in Q$ so, daß

$$(57) \qquad \mathfrak{O}_{\nu\mu} = \gamma_{\nu\mu} \mathfrak{O}_1 \gamma_{\nu\mu}^{-1}$$

gilt; diese $\gamma_{\nu\mu}$ sind bis auf einen rechtsseitigen Faktor ω oder $\zeta\omega$ mit einem willkürlichen $\omega \in k(\mathfrak{O}_1)$ und einem ζ, welches vermöge $\zeta^{-1} k(\mathfrak{O}_1)\, \zeta = k(\mathfrak{O}_1)$ in $k(\mathfrak{O}_1)$ den nicht identischen Automorphismus induziert, durch die $\mathfrak{O}_{\nu\mu}$ festgelegt. Da die $\mathfrak{O}_{\nu\mu}$ in $\mathfrak{J}_\nu$ optimal eingebettet sind, ist jetzt $\mathfrak{O}_1$ in $\gamma_{\nu\mu}^{-1} \mathfrak{J}_\nu \gamma_{\nu\mu} = \mathfrak{J}_{\nu\mu}$ optimal eingebettet. Nach Satz 7 gibt es dann ein $\mathfrak{O}_1$-Ideal $\mathfrak{A}_{\nu\mu}$ derart, daß $\mathfrak{J}_1 \mathfrak{A}_{\nu\mu} = \mathfrak{A}_{\nu\mu} \mathfrak{J}_{\nu\mu}$ ist. Ein Ideal mit denselben Links- und Rechtsordnungen ist aber $\mathfrak{M}_\nu \gamma_{\nu\mu}$. Folglich ist

$$(58) \qquad \mathfrak{J}_1 \mathfrak{A}_{\nu\mu} = \mathfrak{M}_\nu \mathfrak{D}_\nu \gamma_{\nu\mu}$$

mit einem ambigen $\mathfrak{J}_\nu$-Ideal $\mathfrak{D}_\nu$. Dieses schreiben wir in der Form $\mathfrak{D}_\nu = \mathfrak{T}_{\nu\lambda} \delta$, wo $\mathfrak{T}_{\nu\lambda}$ ($\lambda = 1, \ldots, H_\nu$) ein Repräsentantensystem der Klassen ambiger $\mathfrak{J}_\nu$-Ideale ist. Jetzt schreibt sich (58) so:

$$(59) \qquad \mathfrak{J}_1 \mathfrak{A}_{\nu\mu} = \mathfrak{M}_\nu \mathfrak{T}_{\nu\lambda} \delta \gamma_{\nu\mu}.$$

Das Ideal $\mathfrak{A}_{\nu\mu}$ ist seiner Definition (durch Satz 7) gemäß durch die beiden Ordnungen $\mathfrak{J}_1, \mathfrak{J}_{\nu\mu}$ bis auf einen Faktor $\mathfrak{B}$ festgelegt, für den $\mathfrak{J}_1 \mathfrak{B}$ ambig ist. $\mathfrak{B}$ wiederum läßt sich mit einem $\mathfrak{b}$ in k in der Form $\mathfrak{B} = \mathfrak{B}_1 \mathfrak{b}$ schreiben, wobei $\mathfrak{J}_1 \mathfrak{B}_1$ ein ganzes ambiges $\mathfrak{J}_1$-Ideal ist, dessen Norm $\mathfrak{q}$ teilt. Die Anzahl solcher $\mathfrak{B}_1$ ist eine Potenz von 2, die wir am Schluß ermitteln werden; wir bezeichnen sie mit $2^{\varkappa'}$. Mit einem Repräsentantensystem $\mathfrak{a}_\gamma$ ($\gamma = 1, \ldots, h_0$) der $\mathfrak{i}$-Idealklassen kann man endlich $\mathfrak{B} = \mathfrak{B}_1 \mathfrak{a}_\gamma b$, $b \in k$, schreiben. Sind f unter diesen Idealen $\mathfrak{B}_1 \mathfrak{a}_\gamma$ Hauptideale, so verteilen sich die $\mathfrak{B}$ auf $h_0 f^{-1} 2^{\varkappa'}$ Klassen.

Wäre nun $\gamma_{\nu\mu}$ durch $\mathfrak{O}_{\nu\mu}$ nur bis auf einen willkürlichen Faktor $\omega \in k(\mathfrak{O}_1)$ festgelegt, so würden hiernach zu einem $\mathfrak{O}_{\nu\mu}$ genau $h_0 f^{-1} 2^{\varkappa'}$ $\mathfrak{O}_1$-Idealklassen gehören. Weil aber $\gamma_{\nu\mu}$ auch durch $\gamma_{\nu\mu} \zeta\omega$ ersetzt werden kann, so multipliziert sich diese Anzahl noch mit 2, es sei denn, daß zu $\gamma_{\nu\mu}$ und $\gamma_{\nu\mu} \zeta\omega$ äquivalente $\mathfrak{O}_1$-Ideale $\mathfrak{A}_{\nu\mu}$ gehören. Das ist dann und dann der Fall, wenn $\mathfrak{J}_{\nu\mu} \zeta\omega$ für ein geeignetes ω ein ambiges Ideal ist; gilt nämlich (58) und die entsprechende Gleichung $\mathfrak{J}_1 \mathfrak{A}'_{\nu\mu} = \mathfrak{M}_\nu \mathfrak{D}'_\nu \gamma_{\nu\mu} \zeta\omega'$, so folgt aus $\mathfrak{A}'_{\nu\mu} = \mathfrak{A}_{\nu\mu} \omega''$:

$$\gamma_{\nu\mu}^{-1} \mathfrak{D}_\nu'^{-1} \mathfrak{D}_\nu \gamma_{\nu\mu} = \mathfrak{J}_{\nu\mu} \zeta \frac{\omega'}{\omega''}.$$

Das ist ein ambiges Ideal; entsprechend ergibt sich die Umkehrung.

[19]) Die Grundzüge der nachstehenden Überlegung, natürlich ohne Bezugnahme auf die Spur von $P(n)$, finden sich bereits bei *V. Kořínek*, Kvadratická tělesa v kvaternionových okruzích, Věst. Král. Česke Spol. Nauk, Tř. II, 1930, S. 1–46.

Mithin bleibt zu merken: Zu einem $\mathfrak{O}_{\nu\mu}$ gehören $(2)h_0 f^{-1} 2^{\varkappa'}$ $\mathfrak{O}_1$-Idealklassen. Hier ist $(2) = 1$ oder 2, je nachdem es ein $\omega \in k(\mathfrak{O}_1)$ so gibt, daß $\mathfrak{J}_{\nu\mu}\zeta\omega$ ambig ist oder nicht. Ferner ist $2^{\varkappa'}$ die Anzahl der ganzen $\mathfrak{O}_1$-Ideale $\mathfrak{B}_1$ der Art, daß $\mathfrak{J}_1\mathfrak{B}_1$ ambig und $n(\mathfrak{B}_1)$ ein Teiler von $\mathfrak{q}$ ist. Endlich bezeichnet f die Anzahl der Hauptideale der Form $\mathfrak{B}_1\mathfrak{a}_\nu$, wenn $\mathfrak{a}_\nu$ ein Repräsentantensystem der $\mathfrak{i}$-Idealklassen ist.

Wir gehen jetzt umgekehrt von einem $\mathfrak{O}_1$-Ideal $\mathfrak{A}$ aus und suchen der Klasse von $\mathfrak{A}$ eine mit $\mathfrak{O}_1$ isomorphe Ordnung $\mathfrak{O}'$ zuzuordnen. Das Ideal $\mathfrak{J}_1\mathfrak{A}$ ist mit einem der $\mathfrak{M}_\nu\mathfrak{T}_{\nu\lambda}$ linksäquivalent, also

$$\mathfrak{J}_1\mathfrak{A} = \mathfrak{M}_\nu\mathfrak{T}_{\nu\lambda}\gamma_0 = \mathfrak{M}_\nu\mathfrak{T}_{\nu\lambda}\delta\gamma = \mathfrak{M}_\nu\mathfrak{D}_\nu\gamma. \tag{60}$$

Den Faktor γ_0 auf der rechten Seite zerlegen wir auf alle möglichen Weisen in Produkte $\delta\gamma$, wobei $\mathfrak{J}_\nu\delta$ ambig ist. $\mathfrak{O}_1$ ist in der Rechtsordnung dieses Ideals optimal eingebettet und folglich

$$\mathfrak{O}' = \gamma\mathfrak{O}_1\gamma^{-1}$$

in der Rechtsordnung von $\mathfrak{M}_\nu\mathfrak{D}_\nu$, d. h. in $\mathfrak{J}_\nu$. Hiermit sind die Gleichungen (57) bis (59) hergestellt.

Die so dem Ideal $\mathfrak{A}$ zugeordnete Ordnung $\mathfrak{O}'$ hängt ersichtlich nur von der Klasse von $\mathfrak{A}$ ab. Die Anzahl der verschiedenen $\mathfrak{O}'$, die man so erhält, ist gleich der Anzahl der verschiedenen δ in (60) — wobei man jedoch δ und δ' als identisch aufzufassen hat —, für die $\delta^{-1}\mathfrak{O}_1\delta = \delta'^{-1}\mathfrak{O}_1\delta'$ ist. Die δ mit $\delta^{-1}\mathfrak{O}_1\delta = \mathfrak{O}_1$ sind teils die Elemente $\omega \in k(\mathfrak{O}_1)$, teils die $\zeta\omega$, wo ζ die oben erklärte Bedeutung hat. Die δ, für die $\mathfrak{J}_\nu\delta$ ambig ist, bilden eine Gruppe Δ_ν, und die Anzahl der einem γ zugeordneten $\mathfrak{O}'$ ist $\frac{1}{2}[\Delta_\nu : \Delta_\nu \cap k(\mathfrak{O}_1)]$ oder $[\Delta_\nu : \Delta_\nu \cap k(\mathfrak{O}_1)]$, je nachdem ob es ein ambiges Ideal $\mathfrak{J}\zeta\omega$ für die Rechtsordnung $\mathfrak{J}$ von $\mathfrak{J}_1\mathfrak{A}$ gibt oder nicht. Die δ erzeugen innere Automorphismen von $\mathfrak{J}_\nu$; die Anzahl aller inneren Automorphismen von $\mathfrak{J}_\nu$ wurde mit q_ν bezeichnet. Der Index $[\Delta_\nu : \Delta_\nu \cap k(\mathfrak{O}_1)]$ ist gleich q_ν, dividiert durch das Produkt der Anzahl f' der $\mathfrak{O}_1$-Hauptideale $\mathfrak{O}_1\omega$, für die $\mathfrak{J}_1\omega$ ambig ist, mit dem Index $w(\mathfrak{O})$ der Einheitengruppe von $\mathfrak{i}$ in der von $\mathfrak{O}$. Die Anzahl f' stimmt aber mit der bereits oben eingeführten Zahl f überein. Mithin ist

$$[\Delta_\nu : \Delta_\nu \cap k(\mathfrak{O})] = \frac{q_\nu}{f\,w(\mathfrak{O})},$$

und zu einer Klasse gehören genau $\frac{(2)}{2}\,\frac{q_\nu}{f\,w(\mathfrak{O})}$ Ordnungen $\mathfrak{O}'$ in den Ordnungen $\mathfrak{J}_\nu$; das Symbol (2) hat die oben erklärte Bedeutung.

Vergleich der Zuordnungen $\mathfrak{A} \longleftrightarrow \mathfrak{O}$ in beiden Richtungen zeigt nun den folgenden Sachverhalt: Die Klassenzahl $h(\mathfrak{O})$ zerfällt in Summanden h_ν, welche den Ordnungen $\mathfrak{J}_1, \ldots, \mathfrak{J}_T$ zugeordnet sind und bis auf gewisse Faktoren mit den g_ν übereinstimmen. Genauer

$$h(\mathfrak{O}) = \sum_{\nu=1}^{T} h_\nu, \qquad \frac{(2)}{2}\,\frac{q_\nu}{f\,w(\mathfrak{O})}\,h_\nu = (2)\,\frac{h_0\,2^{\varkappa'}}{f}\,g_\nu.$$

Setzt man das Ergebnis in (56) ein, so erhält man

$$Sp(P(\mathfrak{n})) = (M) + \frac{1}{2}\sum_{\mathfrak{O}} 2^{\varkappa-\varkappa'}\,\frac{h(\mathfrak{O})}{w(\mathfrak{O})},$$

d.h. die Behauptung des Satzes 10 bis auf die Bestimmung des Faktors $2^{\varkappa-\varkappa'}$ unter dem Summenzeichen.

Es werde vorausgesetzt, daß für alle unendlichen Primstellen $\mathfrak{o}$ die Artinsymbole $\left(\frac{s, n}{\mathfrak{o}}\right) \neq 1$ sind. Der $2^{\varkappa-\varkappa'}$ entsprechende Faktor in (51) ist nach Satz 7 dann und nur

dann $\neq 0$, wenn es ein $\mathfrak{J}$ der Stufe $\mathfrak{q}$ in Q, d. h. ein $\mathfrak{J}_\nu$ gibt, in dem eine mit $\mathfrak{O}$ isomorphe Ordnung optimal eingebettet ist, und zwar ist dieser Faktor gleich $2^{\varkappa-\varkappa''}$, wo $\varkappa$ die Anzahl der Primfaktoren von $\mathfrak{q}$ und $\varkappa''$ die Anzahl derjenigen $\mathfrak{p} \mid \mathfrak{q}$ ist, für die $\left\{\frac{\mathfrak{O}}{\mathfrak{p}}\right\} = 0$ ist. Es ist zum Beweis von Satz 10 also $\varkappa' = \varkappa''$ zu zeigen. Dieses läuft aber auf die folgende Feststellung hinaus:

Dann und nur dann gibt es ein ganzes $\mathfrak{O}_1$-Ideal $\mathfrak{P}_1$ der Norm $\mathfrak{p}$, für das $\mathfrak{J}_1\mathfrak{P}_1$ ambig ist, wenn $\left\{\frac{\mathfrak{O}_1}{\mathfrak{p}}\right\} = 0$ ist ($\mathfrak{p}$ = Primideal). Die Bedingung $\left\{\frac{\mathfrak{O}_1}{\mathfrak{p}}\right\} = 0$ besagt erstens: $k_\mathfrak{p}(\mathfrak{O}_1)$ ist eine Erweiterung 2. Grades von $k_\mathfrak{p}$, in welcher $\mathfrak{p}$ verzweigt ist, und zweitens: $\mathfrak{O}_{1\mathfrak{p}}$ ist deren Hauptordnung.

$\mathfrak{P}_1$ sei ein ganzes $\mathfrak{O}$-Ideal der Norm $\mathfrak{p}$, und $\mathfrak{J}_1\mathfrak{P}_1$ sei ambig. Da es nur ein einziges ganzes ambiges $\mathfrak{J}_1$-Ideal der Norm $\mathfrak{p}$ gibt, stimmt $\mathfrak{J}_1\mathfrak{P}_1$ mit dem konjugierten Ideal überein und folglich auch $\mathfrak{P}_1$. Aus dem Grunde ist $\mathfrak{p}$ in $k(\mathfrak{O}_1)$ verzweigt, und der Führer von $\mathfrak{O}_{1\mathfrak{p}}$ ist $\mathfrak{i}_\mathfrak{p}$, was zu beweisen war.

Umgekehrt werde $\left\{\frac{\mathfrak{O}_1}{\mathfrak{p}}\right\} = 0$ vorausgesetzt. Dann gibt es ein $\mathfrak{O}_1$-Ideal $\mathfrak{P}_1$ der Norm $\mathfrak{p}$, und dieses stimmt mit dem konjugierten Ideal $\mathfrak{P}_1$ überein. Für $\mathfrak{p} \mid \mathfrak{q}_1$ ist $\mathfrak{J}_{1\mathfrak{p}}$ die einzige maximale Ordnung von $Q_\mathfrak{p}$, und $\mathfrak{J}_{1\mathfrak{p}}\mathfrak{P}_1$ das einzige ambige Ideal der Norm $\mathfrak{p}$. Dann ist auch $\mathfrak{J}_1\mathfrak{P}_1$ ambig. Im Falle $\mathfrak{p} \mid \mathfrak{q}_2$ nehme man $\mathfrak{J}_{1\mathfrak{p}}$ in der Gestalt (2) an und $\mathfrak{O}_{1\mathfrak{p}} = \mathfrak{i}_\mathfrak{p}[\omega]$ mit

$$\omega = \begin{pmatrix} a & b \\ pc & d \end{pmatrix},$$

wobei man $\mathfrak{P}_{1\mathfrak{p}} = \mathfrak{O}_{1\mathfrak{p}}\omega$ voraussetzen darf. Dann ist $ad - pbc \equiv ad \equiv 0 \bmod \mathfrak{p}$. Wegen $\overline{\mathfrak{P}}_1 = \mathfrak{P}_1$ ist $s(\omega) - \omega \equiv \overline{\omega} \equiv 0 \bmod \mathfrak{p}$, also $a + d \equiv 0 \bmod \mathfrak{p}$. Daraus folgt $a \equiv d \equiv 0 \bmod \mathfrak{p}$, und nun ergibt sich aus Satz 5, daß $\mathfrak{J}_1\mathfrak{P}_1$ ambig ist.

Satz 11. *Die Anzahl der Linksidealklassen für eine Ordnung der Stufe* $\mathfrak{q}$ *ist*

$$H = Sp(P(\mathfrak{i})),$$

und die Anzahl der Typen

$$T = 2^{-\varkappa} \sum_{\mathfrak{t} \mid \mathfrak{q}} Sp(P(\mathfrak{t})) = \frac{\sum\limits_{\mathfrak{t} \mid \mathfrak{q}} Sp(P(\mathfrak{t}))}{\sum\limits_{\mathfrak{t} \mid \mathfrak{q}} 1},$$

wo $\varkappa$ *die Anzahl der Primteiler von* $\mathfrak{q}$ *ist.*

Beweis. Die erste Behauptung ist selbstverständlich. Zum Beweis der zweiten gehe man von

$$Sp(P(\mathfrak{t})) = \sum_{\nu=1}^{r} H_\nu \pi_{\nu\nu}(\mathfrak{t}) \tag{61}$$

aus. Die Anzahl der ganzen ambigen $\mathfrak{J}_\nu$-Ideale, deren Normen in $\mathfrak{q}$ aufgehen, ist $2^\varkappa$; die Anzahl der Hauptideale unter ihnen ist $\sum\limits_{\mathfrak{t} \mid \mathfrak{q}} \pi_{\nu\nu}(\mathfrak{t}) = 2^{\lambda_\nu}$. Daher ist $H_\nu = 2^{\varkappa-\lambda_\nu}$. Die Summation von (61) über alle $\mathfrak{t}$ ergibt daher die Typenanzahl, multipliziert mit $2^\varkappa$.

§ 7. Zusammenfassung der Ergebnisse und Folgerungen.

In diesem Paragraphen werden die einschränkenden Voraussetzungen gemacht, daß k der rationale Zahlkörper und $\mathfrak{i}$ die Ordnung der im gewöhnlichen Sinne ganzen rationalen Zahlen sei.

a) Zusammenstellung der Ergebnisse.

Die Diskriminante (der maximalen Ordnungen) der Quaternionen-Algebra Q ist q_1^2, wobei q_1 das Produkt einer ungeraden Anzahl von verschiedenen Primfaktoren ist. Wir betrachten hier i. a. nichtmaximale Ordnungen der Diskriminante $q_1^2 q_2^2$, wobei wir die „Stufe" $q = q_1 q_2$ als quadratfrei voraussetzen. Das Maß ist nach (18)

$$M = \frac{1}{12} \prod_{p \mid q_1} (p-1) \prod_{p \mid q_2} (p+1). \tag{62}$$

Es sei $-d \equiv 1$ oder $\equiv 0 \bmod 4$ eine negative ganze Zahl; sie tritt als Diskriminante der Ordnung $\mathfrak{O} = \left[1, \frac{1+\sqrt{-d}}{4}\right]$ bzw. $[1, \sqrt{-d}]$ aus einem imaginär-quadratischen Zahlkörper oder auch als Diskriminante einer ganzzahligen definiten binären quadratischen Form auf. Mit $h(-d)$ und $w(-d)$ werden die Idealklassenanzahl und die halbe Anzahl der Einheiten von $\mathfrak{O}$ bezeichnet. Es ist also i. a. $w(-d) = 1$, bis auf die Fälle $w(-3) = 3$, $w(-4) = 2$. Zugleich ist $h(-d)$ auch die Anzahl der Klassen primitiver definiter binärer quadratischer Formen der Diskriminante $-d$. Endlich sei

$$\left\{\frac{-d}{p}\right\} = \begin{cases} \left(\frac{-d}{p}\right), & \text{falls } \frac{d}{p^2} \text{ nicht} \\ 1, & \text{falls } \frac{d}{p^2} \end{cases} \equiv 1 \text{ oder } 0 \bmod 4 \text{ ist.}$$

Mit diesen Zeichenerklärungen schreibt sich die Spurformel (51) so:

$$Sp(P(n)) = \tag{63}$$

$$\frac{1}{2} \sum_{s,f} \prod_{p \mid q_1} \left(1 - \left\{\frac{\frac{s^2-4n}{f^2}}{p}\right\}\right) \prod_{p \mid q_2} \left(1 + \left\{\frac{\frac{s^2-4n}{f^2}}{p}\right\}\right) \frac{h\left(\frac{s^2-4n}{f^2}\right)}{w\left(\frac{s^2-4n}{f^2}\right)} + \begin{cases} M & \text{für } n = m^2 \\ 0 & \text{für } n \neq m^2 \end{cases}$$

$$(-2\,|\sqrt{n}\,| < s < 2\,|\sqrt{n}\,|; \quad f > 0; \quad \frac{s^2-4n}{f^2} \equiv 1 \text{ oder } \equiv 0 \bmod 4).$$

Die Klassenanzahl ist nach Satz 11:

$$H = \frac{1}{12} \prod_{p \mid q_1} (p-1) \prod_{p \mid q_2} (p+1) + \frac{1}{4} \prod_{p \mid q_1} \left(1 - \left(\frac{-4}{p}\right)\right) \prod_{p \mid q_2} \left(1 + \left(\frac{-4}{p}\right)\right) + \frac{1}{3} \prod_{p \mid q_1} \left(1 - \left(\frac{-3}{p}\right)\right) \prod_{p \mid q_2} \left(1 + \left(\frac{-3}{p}\right)\right). \tag{64}$$

Die Anzahl der Typen wollen wir nur im Falle $q = p =$ Primzahl angeben, um das Ergebnis mit einem früheren Resultat vergleichen zu können[20]):

$$T = \tfrac{1}{2}\left(\tfrac{1}{2}(h(-4p) + h(-p)) + H\right), \qquad h(-p) = 0, \text{ falls } p \equiv 1 \bmod 4.$$

b) Folgerungen.

Irgendein kommutativer aus gewissen Anzahlmatrizen $P(n)$ erzeugter Ring $\mathfrak{M}$ werde zugrunde gelegt; ein solcher ist z. B. der durch alle $P(n)$ mit $(n, q_2) = 1$ erzeugte

[20]) *M. Deuring*, Die Anzahl der Typen von Maximalordnungen in einer Quaternionenalgebra von primer Grundzahl, Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. 1945, S. 83–85. Dasselbe, J.-ber. Deutsche Math.-Vereing. **54** (1945), S. 24–41 (Druckfehler!).

(Satz 8). Nach Satz 8 ist $\mathfrak{M}$ halbeinfach. $P(n_\gamma)$ mit $\gamma = 1, \ldots, g$ sei eine Basis von $\mathfrak{M}$. Dann ist die Determinante $|Sp(P(n_\mu)\,P(n_\nu))| \neq 0$. Es gibt daher g Matrizen $\widetilde{P}_\mu$ für die

$$Sp(\widetilde{P}_\mu P(n_\nu)) = \begin{cases} 1 & \text{für } \mu = \nu, \\ 0 & \text{für } \mu \neq \nu \end{cases} \tag{65}$$

gilt. Die $\widetilde{P}_\mu$ sind Linearkombinationen

$$\widetilde{P}_\mu = \sum_{\nu=1}^{g} r_{\mu\nu} P(n_\nu). \tag{66}$$

Jede zu $\mathfrak{M}$ gehörige Anzahlmatrix $P(n)$ erlaubt folgende Darstellung durch die Basis:

$$P(n) = \sum_{\nu=1}^{g} \pi_\nu(n)\, P(n_\nu), \tag{67}$$

wobei die Koordinaten wegen (65) und (66)

$$\pi_\mu(n) = Sp(P(n)\,\widetilde{P}_\mu) = \sum_{\nu=1}^{g} r_{\mu\nu} Sp(P(n)\,P(n_\nu)) \tag{68}$$

sind. Mittels der Multiplikationsregeln (24) bis (26) kann man die Produkte $P(n)\,P(n_\nu)$ auf Summen über Anzahlmatrizen $P(m)$ zurückführen und die Koordinaten (68) durch Benutzung von (63) berechnen.

Die Zeilensummen $p(n)$ der Matrizen $P(n)$ sind hiernach ebenfalls durch Klassenzahlsummen ausdrückbar, sobald man die Basis $P(n_\nu)$ kennt. Nach Satz 9 lassen sich die $p(n)$ andererseits elementar berechnen. Der Vergleich beider Ausdrücke liefert dann Relationen für die Idealklassenanzahlen verschiedener imaginär-quadratischer Zahlkörper. Wir werden diese an Hand von einigen Beispielen erläutern.

Es seien p_1, p_2 zwei verschiedene Primzahlen. Wir wollen die Anzahlmatrizen für 4 verschiedene Stufen $q = q_1 q_2$ aufstellen und vergleichen; sie erzeugen also 4 Ringe $\mathfrak{M}_i$, und zwar liege das folgende Schema vor:

	$\mathfrak{M}_1$	$\mathfrak{M}_2$	$\mathfrak{M}_3$	$\mathfrak{M}_4$
q_1	p_1	p_2	p_2	p_1
q_2	1	p_1	1	p_2

Mit den zugehörigen Anzahlmatrizen bilden wir weiter

$$S_1(n) = \begin{pmatrix} P_1(n) & & \\ & P_1(n) & \\ & & P_2(n) \end{pmatrix} \qquad S_2(n) = \begin{pmatrix} P_3(n) & & \\ & P_3(n) & \\ & & P_4(n) \end{pmatrix}.$$

Die $S_1(n)$, $S_2(n)$ erzeugen je einen kommutativen halbeinfachen Ring $\mathfrak{S}_1$, $\mathfrak{S}_2$, wenn alle $P_i(n)$ es tun. Man entnimmt nun der Spurformel (63), daß

$$Sp(S_1(n)) = 2Sp(P_1(n)) + Sp(P_2(n)) = 2Sp(P_3(n)) + Sp(P_4(n)) = Sp(S_2(n))$$

gilt für alle n. Aus der Halbeinfachheit der Ringe $\mathfrak{S}_1$, $\mathfrak{S}_2$ folgt dann, daß die $S_1(n)$ simultan in die $S_2(n)$ transformierbar sind. In diesem Umstand sind noch unbekannte Eigenschaften der Anzahlmatrizen $P(n)$ verborgen. Vielleicht sind diese von der Art, daß man mittels ihrer die „Struktur" der Idealklassen der nicht maximalen Ordnungen von der Struktur der maximalen her übersehen kann?

c) Beispiele.

Sind q_1, q_2 dem nachstehenden Schema entnommen:

q_1	2	3	5	7	13	2	3	2	5	2
q_2	1	1	1	1	1	3	2	5	2	11

so ist die Idealklassenzahl $H = 1$ nach (64). Die Spurformel (63) einerseits und der Satz 9 andererseits ergeben jetzt die Klassenzahlrelationen

$$\frac{1}{2}\sum_{s,f}\left(1-\left\{\frac{\frac{s^2-4n}{f^2}}{q_1}\right\}\right)\left(1+\left\{\frac{\frac{s^2-4n}{f^2}}{q_2}\right\}\right)\frac{h\left(\frac{s^2-4n}{f^2}\right)}{w\left(\frac{s^2-4n}{f^2}\right)}=\left(2\,\frac{q_2^{\alpha_2+1}-1}{q_2-1}-1\right)\prod_{p_\nu}\frac{p_\nu^{\beta_\nu+1}-1}{p_\nu-1}$$

$$\left(-2\,|\sqrt{n}\,|<s<2\,|\sqrt{n}\,|,\ f>0,\ \frac{s^2-4n}{f^2}\equiv 1 \text{ oder } \equiv 0 \bmod 4,\ n=q_1^{\alpha_1}q_2^{\alpha_2}\prod_{p_\nu}p_\nu^{\beta_\nu}+m^2\right).$$

Im Falle $q_1 = 11$, $q_2 = 1$ hat man 2 Klassen und 2 Typen von Ordnungen. Wegen $\left(\frac{-4}{11}\right)=\left(\frac{-3}{11}\right)=-1$ gibt es in Q Einheiten der Ordnungen 4 und 6. Treten beide in einer Ordnung auf, so sind die Einheitenindizes (§ 4) $e_1 \equiv 0 \bmod 12$, $e_2 = 1$; treten sie aber in nicht isomorphen Ordnungen auf, so ist $e_1 = 2$, $e_2 = 3$. Die Anzahlmatrizen $P(n)$ genügen der Symmetriebedingung (22), welche sich jetzt so schreiben läßt: $\pi_{12}(n)\,e_2 = \pi_{21}(n)\,e_1$. Die Zeilensummen von $P(2)$ sind $p(2) = 3$ nach Satz 9. Wäre nun $e_1 \equiv 0 \bmod 12$, $e_2 = 1$, so könnte nur $P(2) = \begin{pmatrix}3&0\\0&3\end{pmatrix}$ sein. Dann enthielte die Ordnung $\mathfrak{J}_2$, welche keine Einheiten $\neq \pm 1$ besitzt, mindestens ein Element α der Norm 2. Dieses ist eine imaginär-quadratische Irrationalität, und daher entweder $\alpha = \pm 1 + \beta$, $\beta^2 = -1$, oder $\alpha^2 = -2$. Das Erstere ist ausgeschlossen, da $\mathfrak{J}_2$ keine Einheiten $\neq \pm 1$ enthält, das zweite ebenso, da $\left(\frac{-2}{11}\right) = 1$ und daher $k(\sqrt{-2})$ nicht Zerfällungskörper von Q ist. Folglich sind die Einheitenindizes $e_1 = 2$, $e_2 = 3$, und aus der Symmetriebedingung sowie den Zeilensummen entnimmt man [21])

$$P(2) = \begin{pmatrix}1&2\\3&0\end{pmatrix}.$$

$P(1)$, $P(2)$ ist eine Basis des Ringes $\mathfrak{M}$ aller Anzahlmatrizen. Die komplementäre Basis ist

$$\tilde{P}_1 = \frac{13}{25}\,P(1) - \frac{1}{25}\,P(2), \qquad \tilde{P}_2 = -\frac{1}{25}\,P(1) + \frac{2}{25}\,P(2).$$

(67), (68) schreiben sich jetzt so:

$$P(n) = \pi_1(n)\,P(1) + \pi_2(n)\,P(2),$$

$$\pi_1(n) = \frac{13}{25}\,Sp(P(n)) - \frac{1}{25}\,Sp(P(n)\,P(2)),$$

$$\pi_2(n) = \frac{-1}{25}\,Sp(P(n)) + \frac{2}{25}\,Sp(P(n)\,P(2)),$$

und das Produkt $P(n)\,P(2)$ ist nach (25):

$$P(n)\,P(2) = P(2n) + 2P\left(\frac{n}{2}\right), \qquad P\left(\frac{n}{2}\right) = 0 \text{ für } \frac{n}{2} \not\equiv 0 \bmod 1.$$

---

[21]) Diskussionen ähnlicher Art erlauben oftmals die Berechnung der $P(n)$ für kleine n und kleine Stufen q, ohne daß man die Ordnungen und Ideale selber aufstellen muß.

Die Zeilensummen sind nun

$$p(n) = \frac{2}{5}\, Sp\,(P(n)) + \frac{1}{5}\, Sp\left(P(2n) + 2P\left(\frac{n}{2}\right)\right) = \prod_{\mathfrak{p}_\nu} \frac{p_\nu^{\beta_\nu+1} - 1}{p_\nu - 1}, \quad n = 11^a \prod_{\mathfrak{p}_\nu} p_\nu^{\beta_\nu}.$$

Setzt man für die Spuren die Werte nach (63) ein, so erhält man Klassenzahlrelationen der 11. Stufe.

Die Einzelausführung der Spurformel und der auf sie aufbauenden Klassenzahlrelationen unter der Voraussetzung, daß $\mathfrak{i}$ eine echte Erweiterung der Ordnung aller ganzen rationalen Zahlen ist (s. § 1), liefert keine neuen Ergebnisse, wie übrigens auch erwartet werden muß.

§ 8. Quaternionen-Algebren über Funktionenkörpern.

Es sei k_0 ein endlicher Körper von q Elementen, die Charakteristik sei $p > 2$. Im folgenden betrachten wir den rationalen Funktionenkörper $k = k_0(\xi)$ einer Unbestimmten ξ. Die Primdivisorzerlegung von ξ ist $\frac{\mathfrak{p}}{\mathfrak{o}}$, und $\mathfrak{o}$ soll der einzige unendliche Primdivisor sein. Dann ist $\mathfrak{i}$ die Ordnung aller Polynome in ξ. Die Einheiten von $\mathfrak{i}$ sind die Konstanten.

Q sei die an den Stellen $\mathfrak{p}$, $\mathfrak{o}$ verzweigte Quaternionen-Algebra über k; sie ist also arithmetisch definit. Wir betrachten die Ordnungen der Stufe $\mathfrak{q} = \mathfrak{p}$, d. h. also die maximalen Ordnungen von Q. Eine von ihnen ist

$$\mathfrak{J} = [1, \iota_1, \iota_2, \iota_3], \quad \iota_1\iota_2 = -\iota_2\iota_1 = \iota_3, \quad \iota_1^2 = \alpha \in k_0, \quad \iota_2^2 = \xi;$$

pabei sei α nicht ein Quadrat in k_0. Man zeigt nun mittels elementarer Schlüsse nach Art der Reduktionstheorie: Eine quaternäre quadratische Form mit Koeffizienten in $\mathfrak{i}$, deren Diskriminante ξ^2 ist, stellt entweder die 0 eigentlich dar oder ist mit $x_1^2 - ax_2^2 - \xi x_3^2 + a\xi x_4^2$ äquivalent. Daraus folgt $H = 1$.

Das aus dem quadratischen Restsymbol abgeleitete Symbol $\left\{\frac{-d}{\mathfrak{p}}\right\}$ hat folgende Bedeutung: Es sei

$$-d = \delta_0 + \delta_1\xi + \cdots + \delta_{2n}\xi^{2n} \qquad \text{(nicht gleichzeitig } \delta_{2n-1} = \delta_{2n} = 0)$$

ein Element in $\mathfrak{i}$. Es ist $\left\{\frac{-d}{\mathfrak{p}}\right\} = 1$, falls entweder δ_0 ein von 0 verschiedenes Quadrat in k_0 oder $\delta_0 = \delta_1 = 0$ ist; $\left\{\frac{-d}{\mathfrak{p}}\right\} = -1$, falls δ_0 ein Nicht-Quadrat in k_0 ist; $\left\{\frac{-d}{\mathfrak{p}}\right\} = 0$, falls $\delta_0 = 0$, $\delta_1 \neq 0$ ist.

Man denke sich $-d$ formal als ein Polynom geraden Grades geschrieben, wie oben. Dann ist $\left(\frac{-d}{\mathfrak{o}}\right) = 0$, wenn $\delta_{2n} = 0$, $\delta_{2n-1} \neq 0$ ist, und $\left(\frac{-d}{\mathfrak{o}}\right) = \pm 1$, je nachdem δ_{2n} ein Quadrat oder ein Nicht-Quadrat in k_0 ist. Bezeichnet n ein Polynom ungeraden Grades in $\mathfrak{i}$, so ist also $\left(\frac{s^2 - 4n}{\mathfrak{o}}\right) \neq 1$ dann und nur dann, wenn der Grad von s höchstens gleich dem halben Grad von n ist.

Aus Satz 9 und der Spurformel (51) folgt nun für ein Polynom $n = n(\xi)$ mit der Primpolynomzerlegung

$$n(\xi) = \prod_\nu p_\nu(\xi)^{\alpha_\nu}, \quad g_\nu = \text{Grad}\,(p_\nu(\xi)), \quad \sum_\nu g_\nu\alpha_\nu \equiv 1 \bmod 2,$$

die Relation

$$\frac{1}{2}\sum_{s,f}\left(1-\left\{\frac{\frac{s^2-4n}{f^2}}{\mathfrak{p}}\right\}\right)h\left(\frac{s^2-4n}{f^2}\right)=\prod_{\nu}\frac{q^{a_\nu+1}-1}{q^{a_\nu}-1};$$

die Summe ist zu erstrecken über alle Polynome $s=s(\xi)$, $f=f(\xi)$ mit

$$\text{Grad}\,(s(\xi))<\frac{1}{2}\,\text{Grad}\,(n(\xi)),\quad \frac{s^2-4n}{f^2}\equiv 0 \bmod \mathfrak{i}.$$

Dabei bedeutet $h\left(\frac{s^2-4n}{f^2}\right)$ die Idealklassenanzahl der Ordnung $\mathfrak{O}=\mathfrak{i}\left[\frac{\sqrt{s^2-4n}}{f}\right]$. Der Einheitenindex $w(\mathfrak{O})$, der in (51) auftritt, ist in diesem Falle durchweg 1.

Da $n(\xi)$ ungeraden Grad haben sollte und in der Relation oben nur Terme mit $\left\{\frac{(s^2-4n)f^{-2}}{\mathfrak{p}}\right\}\neq 1$ auftreten, darf man hier stets s^2-4n von ungeradem Grad voraussetzen. Dann ist $\mathfrak{o}$ in $k(\sqrt{s^2-4n})$ verzweigt. Daraus folgt: Ist $\mathfrak{O}$ die maximale von $\mathfrak{i}$ ganz abhängige Ordnung in $k(\sqrt{s^2-4n})$, d. h. ist $\frac{s^2-4n}{f^2}$ quadratfrei, so ist $h\left(\frac{s^2-4n}{f^2}\right)$ gleich der Anzahl der Divisorenklassen 0. Grades von $k(\sqrt{s^2-4n})$. Es treten mithin in diesen Klassenzahlrelationen u. a. auch Anzahlen von Divisorenklassen 0. Grades auf.

Eingegangen 2. Juli 1954.

Ein Satz über die Menge der vollkommenen Zahlen.

Von *Bodo Volkmann* in Mainz.

1. Wird für jede natürliche Zahl n mit $\sigma(n)$ die Summe ihrer positiven Teiler bezeichnet, so heißt n bekanntlich vollkommen, falls $\sigma(n) = 2n$ ist. Die Menge aller vollkommenen Zahlen sei $\mathfrak{B}$, und ihre Anzahlfunktion, d. h. die Anzahl der Elemente $v \in \mathfrak{B}$ mit $v \leqq x$, werde in der üblichen Weise[1]) mit $V(x)$ bezeichnet. Dann besagt ein kürzlich von Herrn H.-J. Kanold[2]) bewiesener Satz, daß $V(x) = o(x)$ ist. Hauptziel der vorliegenden Arbeit ist es, diese Aussage zu

$$V(x) = O\left(x^{\frac{5}{6}}\right) \tag{1}$$

zu verschärfen. Die dazu erforderlichen Hilfssätze 1 und 2, von denen der erste eine Verallgemeinerung eines Satzes von Herrn Kanold[3]) darstellt, werden, da sie auch unabhängig von der gemachten Anwendung von Interesse sein dürften, gleich in größerer Allgemeinheit bewiesen, als es für den Zweck dieser Arbeit erforderlich wäre. Sie gestatten insbesondere beim Beweis von (1), diese Aussage zugleich auf eine gewisse Menge von mehrfach vollkommenen Zahlen, wie sie Herr Kanold[4]) betrachtet hat, auszudehnen (Satz 1).

2. Für jede natürliche Zahl n und für jedes natürliche $k \geqq 2$ sei die Faktorzerlegung

$$n = t_k(n)\, P_k(n)^k$$

so definiert, daß $t_k(n)$ durch keine k-te Potenz teilbar ist. Dann gilt der

Hilfssatz 1. *Sei $\mathfrak{A}$ eine unendliche Menge von natürlichen Zahlen und $g(x)$ eine für hinreichend große x erklärte, monoton wachsende Funktion, die mit x gegen ∞ strebt derart, daß für jedes $a \in \mathfrak{A}$ die Beziehung*

$$c\, P_k(a)^k \geqq g(a) \qquad (c > 0,\ \textit{reell})$$

gilt. Dann ist $A(x) = o(x)$.

Beweis. Für $a \leqq \frac{x}{c}$ erhält man stets

$$t_k(a)\, g(a) \leqq c\, t_k(a)\, P_k(a)^k = ca \leqq x. \tag{2}$$

Ist $\psi(x)$ eine beliebige monoton wachsende Funktion, die mit x gegen ∞ strebt, so gilt offenbar für hinreichend großes x

---

[1]) Man nennt die Anzahlfunktionen der Mengen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ respektive $A(x)$, $B(x)$, $C(x)$ usw.

[2]) *H.-J. Kanold*, Über die Dichten der Mengen der vollkommenen und der befreundeten Zahlen. Math. Z. 61, 180—185, 1954, Satz 4.

[3]) A. a. O. [2]), Satz 1.

[4]) *H.-J. Kanold*, Über mehrfach vollkommene Zahlen. Journ. reine angew. Math. 194, 218—220, 1955.

$$t_k(a) \begin{cases} \leqq \dfrac{x}{c\psi(x)} & \text{für } a \leqq \dfrac{x}{c\psi(x)} \\ \leqq \dfrac{x}{g\left(\dfrac{x}{c\psi(x)}\right)} & \text{für } \dfrac{x}{c\psi(x)} \leqq a \leqq \dfrac{x}{c}, \end{cases}$$

letzteres wegen $t_k(a)\, g\left(\dfrac{x}{c\psi(x)}\right) \leqq t_k(a)\, g(a) \leqq ca \leqq x$. Somit ist für hinreichend großes x und positives $a \leqq \dfrac{x}{c}$

$$(3) \qquad t_k(a) \leqq \max\left(\frac{x}{c\psi(x)};\ \frac{x}{g\left(\dfrac{x}{c\psi(x)}\right)}\right).$$

Bezeichnet man die rechte Seite von (3) mit $K(x)$, so wird, da es bei festem t höchstens $\left(\dfrac{x}{ct}\right)^{\frac{1}{k}}$ Zahlen a mit $a \leqq \dfrac{x}{c}$ und $t_k(a) = t$ gibt,

$$(4) \qquad A(x) \leqq c' + \sum_{t=1}^{[K(x)]} \left(\frac{x}{ct}\right)^{\frac{1}{k}} = O\left(x^{\frac{1}{k}} \int_0^{K(x)} t^{-\frac{1}{k}}\, dt\right) = O\left(x^{\frac{1}{k}} K(x)^{\frac{k-1}{k}}\right) \qquad (c' > 0)$$

und folglich $\dfrac{A(x)}{x} = O\left(\left(\dfrac{K(x)}{x}\right)^{\frac{k-1}{k}}\right)$, also $A(x) = o(x)$.

Unter den Voraussetzungen von Hilfssatz 1 gilt der

Hilfssatz 2. a) *Ist* $g(x) = x^{\alpha}$ $(0 < \alpha < 1)$, *so wird*

$$A(x) = O\left(x^{1 - \frac{\alpha}{1+\alpha} \cdot \frac{k-1}{k}}\right).$$

b) *Ist* $g(x) = \log^{\tau_1} \log^{\tau_2} \cdots \log^{\tau_q} x$ $(\tau_1, \ldots, \tau_q > 0,\ q \geqq 1)$, *so ist*

$$A(x) = O\left(x (\log^{\tau_1} \log^{\tau_2} \cdots \log^{\tau_q} x)^{\frac{1-k}{k}}\right).$$

Beweis. a) Setzt man $\psi(x) = x^{\frac{\alpha}{1+\alpha}}$, so werden beide bei der Definition (3) von $K(x)$ auftretenden Ausdrücke einander asymptotisch proportional, nämlich — von konstanten Faktoren abgesehen — gleich $x^{\frac{1}{1+\alpha}}$, und daher erreicht das Maximum $K(x)$ in diesem Falle seine kleinstmögliche Größenordnung. Man erhält somit nach (4), wie behauptet,

$$A(x) = O\left(x^{\frac{1}{k}} K(x)^{\frac{k-1}{k}}\right) = O\left(x^{\frac{1}{k} + \frac{1}{1+\alpha} \cdot \frac{k-1}{k}}\right) = O\left(x^{1 - \frac{\alpha}{1+\alpha} \cdot \frac{k-1}{k}}\right).$$

b) Setzt man $\psi(x) = g(x)$, so erhält man wie bei a) asymptotische Proportionalität von $\dfrac{x}{c\psi(x)}$ mit $\dfrac{x}{g\left(\dfrac{x}{c\psi(x)}\right)}$; denn es besteht die asymptotische Gleichung

$$\frac{x}{g\left(\dfrac{x}{c\psi(x)}\right)} = \frac{x}{\log^{\tau_1} \log^{\tau_2} \cdots \log^{\tau_q} (x - c \log^{\tau_1} \cdots \log^{\tau_q} x)}$$

$$\cong \frac{x}{\log^{\tau_1} \cdots \log^{\tau_q} x} = \frac{x}{\psi(x)}.$$

Damit wird nach (4)

$$A(x) = O\left(x(\log^{\tau_1} \cdots \log^{\tau_q} x)^{\frac{k-1}{k}}\right).$$

3. Eine Zahl n heißt mehrfach vollkommen, wenn $n \mid \sigma(n)$ und $\frac{\sigma(n)}{n} > 2$ ist. Wir betrachten für jede natürliche Zahl i speziell die Menge $\mathfrak{U}_i$ der ungeraden Zahlen n mit

$$\sigma(n) = 2^i n, \tag{5}$$

die somit im Falle $i > 1$ mehrfach vollkommen sind und im Falle $i = 1$ die ungeraden vollkommenen Zahlen darstellen. Dann gilt der

Satz 1. *Für die Menge $\mathfrak{U}_i$ ist $U_i(x) = O\left(x^{1-\frac{1}{2(i+2)}}\right)$ $(i = 1, 2, \ldots)$.*

Zum Beweis benötigen wir den von Herrn Kanold[5]) bewiesenen

Hilfssatz 3. *Sei $n > 6$ vollkommen oder mehrfach vollkommen und p der größte Primteiler von n. Dann ist*

$$P_2(n)^2 \geqq \frac{p+1}{2}.$$

Beweis von Satz 1. Nach (5) ist für jedes $n \in \mathfrak{U}_i$, wenn die Primfaktorzerlegung in der Form $n = \prod_{\lambda=1}^{l} p_\lambda^{\beta_\lambda}$ geschrieben wird,

$$\sigma(n) = \prod_{\lambda=1}^{l} (1 + p_\lambda + \cdots + p_\lambda^{\beta_\lambda}) = 2^i \prod_{\lambda=1}^{l} p_\lambda^{\beta_\lambda}.$$

Da die Primzahl 2 in der linken Seite genau in der i-ten Potenz aufgeht, jedoch alle p_λ ungerade sind, muß für eine gewisse Anzahl j (mit $1 \leqq j \leqq i$) von Indizes

$$2 \mid (1 + p_\lambda + \cdots + p_\lambda^{\beta_\lambda}), \tag{6}$$

also β_λ ungerade sein, und für alle übrigen λ ist dann β_λ gerade. Wir erreichen durch geeignete Numerierung, daß (6) für $\lambda = 1, \ldots, j$ gilt. Dann ist, wenn $\prod_{\lambda=1}^{j} p_\lambda = f$ gesetzt wird, n von der Form $n = fm^2$ mit natürlichem m. Somit wird $m^2 = P_2(n)^2$, und nach Hilfssatz 3 ist folglich, falls $n > 6$ ist, $m^2 \geqq \frac{p+1}{2}$, also

$$f = \frac{n}{m^2} \leqq \frac{2n}{p+1} = \frac{2fm^2}{p+1} < \frac{2fm^2}{f^{\frac{1}{j}}} = 2f^{1-\frac{1}{j}} m^2,$$

d. h. $f^{\frac{1}{j}} \leqq 2m^2$, damit $f^{1+\frac{1}{j}} \leqq 2fm^2 = 2n$ und schließlich $f \leqq (2n)^{\frac{j}{j+1}} \leqq (2n)^{\frac{i}{i+1}}$, woraus $m^2 = \frac{n}{f} \geqq 2^{-\frac{i}{i+1}} n^{\frac{1}{i+1}}$ folgt.

Daher werden die Hilfssätze 1 und 2a) mit $k = 2$, $P_2(n)^2 = m^2$, $c = 2^{\frac{i}{i+1}}$ und $\alpha = \frac{1}{i+1}$ auf die Menge $\mathfrak{U}_i$ anwendbar, und man erhält somit

$$U_i(x) = O\left(x^{1-\frac{1}{2(i+2)}}\right) \qquad (i = 1, 2, \ldots).$$

---

[5]) A. a. O. [4]), Satz 1. Wir beschränken uns hier auf einen Teil der dortigen Aussage.

Satz 2. ***Für die Menge $\mathfrak{V}$ der vollkommenen Zahlen gilt***

$$V(x) = O\left(x^{\frac{5}{6}}\right).$$

Beweis. **a) Für die Menge $\mathfrak{U}_1$ der ungeraden vollkommenen Zahlen gilt nach Satz 1**

$$U_1(x) = O\left(x^{\frac{5}{6}}\right). \tag{7}$$

b) Da jede gerade vollkommene Zahl nach Euler*) von der Form

$$g = 2^q(2^{q+1} - 1) \qquad (q + 1 = \text{Primzahl})$$

ist, gilt für die Menge $\mathfrak{G} = \{g_1, g_2, \ldots\}$ aller geraden vollkommenen Zahlen, wenn die g_t der Größe nach geordnet sind, sicher

$$g_t > 4^t \quad (t = 1, 2, \ldots),$$

also

$$G(x) < \frac{\log x}{\log 4}. \tag{8}$$

Aus (7) und (8) folgt die Behauptung wegen $\mathfrak{V} = \mathfrak{U}_1 \vee \mathfrak{G}$.

***) Siehe z. B. *E. Trost*, Primzahlen, Verlag Birkhäuser, Basel 1953, Seite 35.**

Eingegangen 12. Juli 1954.

Druckfehlerberichtigung zu

Rohrbach und Volkmann, Verallgemeinerte asymptotische Dichten

(dieses Journal 194, 195—209, 1955).

Die Zeile vor Hilfssatz 13 (Seite 205, Zeile 4 v. u.) ist dort zu streichen und auf Seite 208 zwischen Zeile 14 und Zeile 15 einzufügen.

Über die Darstellbarkeit von Modulformen durch Thetareihen.

Von *Martin Eichler* in Münster.

Einleitung.

Die von Hecke in die Theorie der Modulformen eingeführten Operatoren T_n gestatten bekanntlich Anwendungen auf die Frage nach der Darstellung von Zahlen durch definite quadratische Formen gerader Variablenzahl. Hierbei steht allerdings der Umstand hindernd im Wege, daß man i. a. nicht weiß, welche Modulformen eines vorgelegten Typus durch Thetareihen zu quadratischen Formen darstellbar sind. Infolgedessen bedarf die Heckesche Theorie in diesem Zusammenhang der Ergänzung durch rein zahlentheoretische Methoden aus der Theorie der quadratischen Formen.

Wie ich kürzlich hervorhob[1]), sind die T_n im Bereich der Spitzenformen (-2)-ten Grades Darstellungen von Multiplikatoren des Körpers der Modulfunktionen in sich. Damit entsteht die Aufgabe, sie auch vom Standpunkt der algebraischen Funktionen her zu beleuchten. Diese Aufgabe ist allein schon deshalb wichtig, weil man außer den Körpern der Modulfunktionen bisher erst wenige Beispiele von Funktionenkörpern besitzt, welche nichttriviale Multiplikatoren zulassen.

In dieser Arbeit werde ich nun, in Umkehrung der Blickrichtung Heckes, Ergebnisse der Arithmetik der quadratischen Formen (bzw. der ihnen zugrunde liegenden Quaternionen-Algebren) heranziehen, um Eigenschaften der T_n herzuleiten. Das Hauptresultat, Satz 1 in § 4, bestätigt eine Vermutung Heckes aus dem Jahre 1936 über die Darstellbarkeit aller ganzen Modulformen (-2)-ten Grades von Primzahlstufe und Haupttypus durch Thetareihen[2]). Satz 2 enthält eine Verallgemeinerung, stellt aber gleichzeitig fest, daß es bei zusammengesetzter Stufe Modulformen gibt, welche durch Thetareihen nicht dargestellt werden können, was meines Wissens bisher nur vermutet wurde.

Die Methode besteht in dem Vergleich der Darstellungen der T_n einerseits im Raume aller Spitzenformen und andererseits in dem Teilraume, dessen Elemente durch Differenzen von Thetareihen darstellbar sind. Von beiden Darstellungen wird die Spur ermittelt. Die Berechnung der letzteren Spur ist im Prinzip in einer früheren Arbeit enthalten[3]), die Berechnung der ersteren erfolgt hier durch Heranziehung von Sätzen über die Korrespondenzen algebraischer Funktionenkörper.

---

[1]) *M. Eichler*, Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, Arch. d. Math. 5 (1954), S. 355–366.

[2]) *E. Hecke*, Analytische Arithmetik der positiven quadratischen Formen, Kgl. Danske Videnskabernes Selskab, Math.-fys. Medd. XVII, 12 (1940), S. 100.

[3]) *M. Eichler*, Zur Zahlentheorie der Quaternionen, dies Journ. 195 (1955), 127–151.

Im einzelnen ist über den Inhalt noch folgendes zu sagen. Betrachtet werden ausschließlich Modulfunktionen $\varphi(\tau)$, welche bei der Gruppe

$$\Gamma_0(q): \quad \tau \to \frac{a\tau + b}{qc\tau + d}, \qquad \begin{vmatrix} a & b \\ qc & d \end{vmatrix} = 1, \quad a, b, c, d \equiv 0 \bmod 1$$

invariant bleiben, sowie entsprechende Modulformen. *Über die Stufe q wird vorausgesetzt, daß sie quadratfrei sei.* Die bei $\Gamma_0(q)$ invarianten Funktionen bilden einen algebraischen Funktionenkörper K über dem Körper k aller komplexen Zahlen. § 1 bringt Grundbegriffe und Bezeichnungen. In § 2 und 3 wird die Spur der T_n im Raume der Spitzenformen (-2)-ten Grades ermittelt. In § 4 erfolgt der Vergleich der beiden oben genannten Spuren, die in der Hauptsache Klassenzahlsummen von der Art sind, wie sie in den bekannten Relationen zwischen den Klassenzahlen definiter binärer quadratischer Formen auftreten. Die naheliegende Frage, in welchem Verhältnis die vorliegende Arbeit mit den älteren Arbeiten über Klassenzahlrelationen und Modularkorrespondenzen, insbesondere von Hurwitz, steht, wird in § 5 beantwortet. Schließlich wird in § 6 gezeigt, daß auch i. a. alle ganzen Modulformen $(-2k)$-ten Grades $(k = 2, 3, \ldots)$ von Primzahlstufe und Haupttypus durch Thetareihen darstellbar sind, was sich als eine Folge aus dem entsprechenden Sachverhalt für $k = 1$ (Satz 1) ergibt.

§ 1. Die Modularkorrespondenzen τ_n, $(n, q) = 1$.

Im folgenden bedeute n stets eine natürliche zur Stufe q teilerfremde Zahl. Die Matrizen

$$(1) \qquad \begin{pmatrix} s & r \\ 0 & t \end{pmatrix} \text{ mit } st = n,\ s > 0,\ (r, s, t) = 1,\ 0 \leqq r < t$$

bilden bekanntlich ein Vertretersystem für die Klassen nach $\Gamma_0(q)$ linksseitig assoziierter primitiver Matrizen der Determinante n und der Form

$$\begin{pmatrix} a & b \\ qc & d \end{pmatrix}, \quad a \equiv b \equiv c \equiv d \equiv 0 \bmod 1.$$

Daher sind mit einer Modulfunktion $\varphi(\tau)$ auch die symmetrischen Funktionen der $\varphi\left(\frac{s\tau + r}{t}\right)$ bei $\Gamma_0(q)$ ivariant.

Bezeichnet $\sigma(\tau)$ eine Spitzenform (-2)-ten Grades zu $\Gamma_0(q)$, so ist $\sigma(\tau)\,d\tau$ ein Differential 1. Gattung des Körpers K. Summiert man über die Matrizen (1), so erhält man bekanntlich in folgender Weise ein weiteres mit $(\sigma(\tau) \mid \overline{\tau}_n)\,d\tau$ bezeichnetes Differential 1. Gattung:

$$(2) \qquad \sum_{r,s,t} \sigma\left(\frac{s\tau + r}{t}\right) d\left(\frac{s\tau + r}{t}\right) = \sum_{r,s,t} \frac{s}{t} \sigma\left(\frac{s\tau + r}{t}\right) d\tau = (\sigma(\tau) \mid \overline{\tau}_n)\,d\tau.$$

Der hiermit definierte Operator $\overline{\tau}_n$ (wir benutzen in Abweichung von Hecke einen griechischen Buchstaben) erfährt unter Benutzung einer Basis $\sigma_i(\tau)$ $(i = 1, \ldots, g =$ Geschlecht von $K)$ der Schar der Spitzenformen eine Darstellung

$$(3) \qquad \sigma_i(\tau) \mid \overline{\tau}_n = \sum_{k=1}^{g} \overline{t}_{ik}(n)\, \sigma_k(\tau)$$

durch g-reihige Matrizen $\overline{T}_n = (\overline{t}_{ik}(n))$. Formale Addition der $\overline{\tau}_n$ liefert den bekannten Heckeschen Operator

$$(4) \qquad \tau_n = \sum_{\nu^2 \mid n} \overline{\tau}_{n\nu^{-2}}.$$

An seiner Stelle werden wir im folgenden allerdings hauptsächlich den Operator

$$\tau_n^0 = \sum_{\substack{\nu^2 \mid n \\ \nu^2 \neq n}} \bar{\tau}_{n\nu^{-1}} \tag{5}$$

benutzen, der sich von τ_n nur für quadratisches n unterscheidet. Die entsprechenden Bildungen für die Darstellung (2), (3) bezeichnen wir mit T_n, T_n^0.

Die Gleichungen (2), (3) definieren die Darstellung T_n^0 eines Multiplikators τ_n^0 von K zu sich im Raume der Differentiale 1. Gattung. Dieser Multiplikator wird durch eine Korrespondenz (Modularkorrespondenz) von K zu einem isomorphen Körper K' wie folgt erzeugt[4]). K' sei der Körper der bei $\Gamma_0(q)$ invarianten Funktionen einer von τ unabhängigen Variablen τ'. Man bilde zunächst den Integritätsbereich $\mathfrak{J} = KK'$, nämlich die Gesamtheit der Ausdrücke $\varphi_1 \varphi_1' + \varphi_2 \varphi_2' + \cdots$, $\varphi_\nu \in K$, $\varphi_\nu' \in K'$. Man bilde weiter das ganze $\mathfrak{J}$-Ideal

$$\mathfrak{T}_n^0 = \mathfrak{J}\left\{ \prod_{r,s,t} \left(\varphi(\tau) - \varphi\left(\frac{s\tau' + r}{t}\right)\right)\right\}, \tag{6}$$

das folgendermaßen zu verstehen ist: Das Produkt wird für je eine Funktion $\varphi \in K$ gebildet und über alle Matrizen

$$\begin{pmatrix} s & r \\ 0 & t \end{pmatrix} \text{ mit } st = n,\ s > 0,\ 0 \leqq r < t, \text{ ausgenommen } s = t = \sqrt{n},\ r = 0 \tag{7}$$

erstreckt; $\mathfrak{T}_n^0$ ist das aus allen diesen Produkten erzeugte $\mathfrak{J}$-Ideal. Es definiert nun eine Korrespondenz von K zu K' und seine Klasse den Multiplikator τ_n^0.

Die Multiplikatoren von K lassen sich in der Jacobischen Mannigfaltigkeit darstellen, und die Spur dieser Darstellung ist doppelt so groß wie die der Darstellung (2), (3), falls diese letztere reell ist, und das trifft hier zu. Für sie hat Hurwitz den folgenden wichtigen Satz bewiesen[5]), auf den sich alles weitere hier stützen wird:

$$Sp(T_n^0) = \tfrac{1}{2}(d_n^0 + d_n^{0\prime} - c_n^0), \tag{8}$$

wo d_n^0 und $d_n^{0\prime}$ die Grade von $\mathfrak{T}_n^0$ als Divisoren des Körperkompositums $\mathfrak{K} = KK'$ über K' und K bedeuten (wie das gemeint ist, braucht nicht näher ausgeführt zu werden) und c_n^0 die sogenannte Koinzidenzenanzahl, deren Definition unten folgt.

Der Divisorgrad d_n^0 ist gleich der Anzahl der Faktoren in (6). Der Divisorgrad $d_n^{0\prime}$ ist ebenso groß; das folgt sofort aus der Invarianz von $\mathfrak{T}_n^0$ bei der Vertauschung von K und K':

$$\mathfrak{T}_n^{0\prime} = \mathfrak{T}_n^0. \tag{9}$$

Zum Beweise von (9) stellen wir zunächst fest, daß das entsprechend (6) mit allen Matrizen (1) gebildete $\mathfrak{J}$-Ideal $\bar{\mathfrak{T}}_n$ ein Primideal ist, denn nicht für jede Funktion $\varphi \in K$ sind schon alle symmetrischen Funktionen der $\varphi\left(\frac{s\tau + r}{t}\right)$ für ein echtes Teilsystem von (1) wieder bei $\Gamma_0(q)$ invariant. Nun ist $\tau_0' = \tau_0 n$ nach (6) Bildpunkt von τ_0 bei der Korrespondenz $\bar{\mathfrak{T}}_n$. Also ist umgekehrt $\tau_0 = \tau_0' n^{-1}$ Bildpunkt von τ_0' bei der Korrespondenz $\bar{\mathfrak{T}}_n'$. Als $\mathfrak{J}$-Ideal enthält demnach diese Korrespondenz den Faktor $\mathfrak{J}\left\{\varphi(\tau) - \varphi\left(\frac{\tau'}{n}\right)\right\}$; wegen der Prim-

---

[4]) Zur Theorie der Korrespondenzen und Multiplikatoren algebraischer Funktionenkörper vgl. etwa *M. Deuring*, Arithmetische Theorie algebraischer Funktionenkörper, Teil I., dies Journ. 177 (1937), S. 161–191; Teil II., ebenda 183 (1940), S. 25–36.

[5]) *A. Hurwitz*, Über algebraische Korrespondenzen und das verallgemeinerte Korrespondenzprinzip, Math. Annalen 28 (1887), S. 561–585 = Math. Werke I, Basel 1933, S. 179, Formel (29).

idealeigenschaft von $\mathfrak{T}_n$ ist daher $\overline{\mathfrak{T}}_n$ ein Teiler von $\overline{\mathfrak{T}}'_n$. Mithin muß $\overline{\mathfrak{T}}'_n = \overline{\mathfrak{T}}_n$ sein. Die Gleichung (9) folgt hieraus durch die (5) entsprechende Produktbildung. Aus (9) aber folgt, wie gesagt,

$$(10) \qquad d_n^0 = d_n^{0\prime} = \sum_{t|n} t - \begin{cases} 0 \text{ für } \sqrt{n} \not\equiv 0 \bmod 1, \\ 1 \text{ für } \sqrt{n} \equiv 0 \bmod 1. \end{cases}$$

So groß ist nämlich die Anzahl der Faktoren in (6).

Zur Definition der Koinzidenzenanzahl c_n^0 sei $\mathfrak{p}$ ein Punkt von K und $\mathfrak{p}'$ der $\mathfrak{p}$ bei der natürlichen Isomorphie entsprechende Punkt von K'. Ferner seien $\mathfrak{i}_\mathfrak{p}, \mathfrak{i}'_{\mathfrak{p}'}$ die Integritätsbereiche der in $\mathfrak{p}, \mathfrak{p}'$ ganzen Funktionen von K, K' und $\mathfrak{J}_\mathfrak{p} = \mathfrak{i}_\mathfrak{p}\mathfrak{i}'_{\mathfrak{p}'}$ der $\mathfrak{J}$ analog gebildete und in $\mathfrak{J}$ enthaltene Integritätsbereich. Identifiziert man nun in dem $\mathfrak{J}_\mathfrak{p}$-Ideal $\mathfrak{J}_\mathfrak{p} \cap \mathfrak{T}_n^0$ die Integritätsbereiche $\mathfrak{i}_\mathfrak{p}$ und $\mathfrak{i}'_{\mathfrak{p}'}$ elementweise, so entsteht ein ganzes $\mathfrak{i}_\mathfrak{p}$-Ideal $\mathfrak{t}_{n,\mathfrak{p}}^0$, das demnach eine Potenz des zu $\mathfrak{p}$ gehörigen und ebenfalls mit $\mathfrak{p}$ bezeichneten einzigen $\mathfrak{i}_\mathfrak{p}$-Ideals ist: $\mathfrak{t}_{n,\mathfrak{p}}^0 = \mathfrak{p}^{h_\mathfrak{p}}$. Der Exponent $h_\mathfrak{p}$ ist die Koinzidenzmultiplizität von $\mathfrak{p}$, und c_n^0 die Summe der $h_\mathfrak{p}$ für alle Punkte $\mathfrak{p}$ von K.

Diese Definition versagt für die Einheits-Korrespondenz

$$\mathfrak{T}_1 = \mathfrak{J}\{\varphi(\tau) - \varphi(\tau')\},$$

da dann $\mathfrak{t}_{1,\mathfrak{p}} = 0$ wird. Man setzt jetzt die Koinzidenzenanzahl $c_1 = -2(g-1)$ an, wo g das Geschlecht von K ist. Dann wird $Sp(T_1) = g$ in Übereinstimmung mit (8).

Man kann c_n^0 offenbar auch so bekommen: $\mathfrak{i}_\mathfrak{p}$ wird durch den Integritätsbereich $\mathfrak{i}_0$ aller derjenigen Funktionen von K ersetzt, die überall, von einer endlichen Menge von Punkten $\mathfrak{p}_\nu$ abgesehen, endlich sind. Dann ist c_n^0 gleich dem Grad $c_{n,0}^0$ des $\mathfrak{i}_0$-Ideals $\mathfrak{t}_{n,0}^0 = \mathfrak{i}_0\mathfrak{i}'_0 \cap \mathfrak{T}_n^0$ vermehrt um die Summe $c_{n,\infty}^0$ der Koinzidenzmultiplizitäten der Ausnahmepunkte $\mathfrak{p}_\nu$:

$$(11) \qquad c_n^0 = c_{n,0}^0 + c_{n,\infty}^0.$$

§ 2. Die Anzahl der endlichen Koinzidenzpunkte.

Die Anzahl c_n^0 wird nun auf der Basis der Zerlegung (11) berechnet, und zwar werden die rationalen Spitzen des Fundamentalbereichs von $\Gamma_0(q)$ als die Ausnahmepunkte $\mathfrak{p}_\nu$ genommen. In § 2 wird zunächst $c_{n,0}^0$ berechnet. Dabei muß ein Unterschied zwischen den inneren Punkten des Fundamentalbereichs und dessen elliptischen Ecken gemacht werden.

Es sei τ_0 ein Punkt im Inneren der oberen Halbebene, jedoch nicht eine elliptische Ecke, dem eine positive Koinzidenzmultiplizität zukommt. Dann gilt

$$\frac{s\tau_0 + r}{t} = \frac{a\tau_0 + b}{qc\tau_0 + d}, \qquad \begin{pmatrix} a & b \\ qc & d \end{pmatrix} \in \Gamma_0(q), \qquad \operatorname{Im}(\tau_0) > 0,$$

wobei r, s, t den Bedingungen in (7) genügen; τ_0 darf aber nicht Fixpunkt einer Substitution aus $\Gamma_0(q)$ sein. Man kann diese Bedingung auch so schreiben:

$$(12) \quad N(\tau_0) = \frac{A\tau_0 + B}{qC\tau_0 + D} = \tau_0, \; |N| = \begin{vmatrix} A & B \\ qC & D \end{vmatrix} = n, \; (A, B, C, D) \neq \sqrt{n}, \; \operatorname{Im}(\tau_0) > 0.$$

Die Gesamtheit aller Substitutionen N, die τ_0 fest lassen, entstehen aus einer festen durch Multiplikation mit einem Faktor und Addition eines Vielfachen der Einheitsmatrix. Daß τ_0 nicht eine elliptische Ecke ist, kommt demnach folgendermaßen zum Ausdruck:

$$(12a) \qquad N \neq u + vU, \; U \in \Gamma_0(q), \; u, v \text{ ganz rational.}$$

Daß u und v ganz rational sein sollen, bedeutet offenbar keine Einschränkung. Hier ist u als Abkürzung des u-fachen der Einheitsmatrix zu verstehen.

Die Vielfachheit von τ_0 als Koinzidenzpunkt ist offenbar 1, da $\tau - \tau_0$ ortsuniformisierend ist.

Ersetzt man N durch $U^{-1}NU$, $U \in \Gamma_0(q)$, so geht τ_0 in den äquivalenten Punkt $U(\tau_0)$ über. Die Anzahl $c^0_{n,0,0}$ der nicht in elliptischen Ecken liegenden Koinzidenzpunkte ist demnach gleich der Anzahl der Klassen „nach $\Gamma_0(q)$ konjugierter" Substitutionen $U^{-1}NU$, die den Bedingungen in (12), (12a) genügen.

Zur Bestimmung dieser Anzahl werden folgende Eigenschaften der Ordnung $\mathfrak{O}$ aller Matrizen $\begin{pmatrix} a & b \\ qc & d \end{pmatrix}$ mit ganzen rationalen a, b, c, d benutzt.

1) Jedes Links- oder Rechtsideal für $\mathfrak{O}$ ist Hauptideal[6]).

2) Zu jedem Primteiler p von q gibt es genau ein ganzes ambiges $\mathfrak{O}$-Ideal der Norm p, repräsentiert etwa durch

$$P_p = \begin{pmatrix} pa & -1 \\ qc & p \end{pmatrix}, \qquad pa + \frac{q}{p}c = 1\ ^{7}).$$

3) Alle ambigen $\mathfrak{O}$-Ideale sind von der Form $\mathfrak{O} P_{p_1}^{\varepsilon_1} P_{p_2}^{\varepsilon_2} \cdots r$, $p_i \mid q$, $\varepsilon_i = 0$ oder 1, r eine rationale Zahl. Die Reihenfolge der Faktoren ist gleichgültig. Bei ganzen primitiven ambigen Idealen ist $r = 1$; die Anzahl von diesen ist also $2^\varkappa$, wo $\varkappa$ die Anzahl der Primfaktoren von q bedeutet.

4) Eine Ordnung $\mathfrak{O}$ eines durch zweireihige Matrizen dargestellten quadratischen Zahlkörpers Z heißt in $\mathfrak{O}$ optimal eingebettet, wenn $\mathfrak{O} = \mathfrak{O} \cap Z$ ist. Notwendig und hinreichend für die Existenz einer in $\mathfrak{O}$ optimal eingebetteten Ordnung $\mathfrak{O}$, welche mit einer abstrakt vorgegebenen Ordnung $\mathfrak{O}_0$ eines quadratischen Zahlkörpers Z_0 isomorph ist, ist daß das Produkt

$$\prod_{p \mid q} \left(1 + \left\{\frac{\Delta(\mathfrak{O}_0)}{p}\right\}\right) \tag{13}$$

nicht verschwindet. Dabei ist das Symbol $\left\{\frac{\Delta(\mathfrak{O}_0)}{p}\right\}$ für die Diskriminante $\Delta(\mathfrak{O}_0)$ durch das Legendresymbol folgendermaßen definiert:

$$\left\{\frac{\Delta}{p}\right\} = \begin{cases} \left(\frac{\Delta}{p}\right), & \text{falls } \Delta p^{-2} \not\equiv 0 \text{ oder } 1 \bmod 4, \\ 1, & \text{falls } \Delta p^{-2} \equiv 0 \text{ oder } 1 \bmod 4. \end{cases} \tag{14}$$

5) Es sei p ein Primteiler von q, $\mathfrak{O}$ eine in $\mathfrak{O}$ optimal eingebettete Ordnung und $\left\{\frac{\Delta(\mathfrak{O})}{p}\right\} = 0$. Dann gibt es ein ganzes $\mathfrak{O}$-Ideal $\mathfrak{B}$ der Norm p, und $\mathfrak{A} = \mathfrak{O}\mathfrak{B}$ ist das ganze ambige $\mathfrak{O}$-Ideal der Norm p.

6) Ist $\mathfrak{O}$ in den beiden Ordnungen $\mathfrak{O}$ und $\mathfrak{O}_1 = V^{-1}\mathfrak{O}V$ optimal eingebettet, so gibt es ein $\mathfrak{O}$-Ideal $\mathfrak{B}$ so, daß $\mathfrak{O}\mathfrak{B}$ die Rechtsordnung $\mathfrak{O}_1$ hat. Ist umgekehrt $\mathfrak{B}$ ein $\mathfrak{O}$-Ideal, so ist $\mathfrak{O}$ auch in der Rechtsordnung von $\mathfrak{O}\mathfrak{B}$ optimal eingebettet.

Eine Substitution N der Art (12), (12a) sei vorgelegt. Ihre Spur und Norm (Determinante) werden

$$Sp(N) = A + D = \sigma, \quad n(N) = AD - qBC = n$$

geschrieben. Die Diskriminante ist $\Delta(N) = \sigma^2 - 4n < 0$ wegen $\mathrm{Im}(\tau_0) > 0$. Die Substitution N erzeugt daher einen (imaginär-)quadratischen Zahlkörper Z, die Ordnung

[6]) Das ist leicht elementar beweisbar. Die Behauptung ist ein Spezialfall eines wesentlich allgemeineren Satzes in: *M. Eichler*, Die Ähnlichkeitsklassen indefiniter Gitter, Math. Zeitschr. **55** (1952), S. 216–252.

[7]) Die folgenden Aussagen finden sich sämtlich unter [3]), § 1–3.

$\mathfrak{O} = \mathfrak{Q} \cap Z$ ist in $\mathfrak{Q}$ optimal eingebettet. Hiermit ist N in eindeutiger Weise eine in $\mathfrak{Q}$ optimal eingebettete Ordnung $\mathfrak{O}$ zugeordnet worden. Umgekehrt ist aber N auch in einer solchen Ordnung durch Spur und Norm in eindeutiger Weise gekennzeichnet. Für die Diskriminante von $\mathfrak{O}$ gilt dann mit einer natürlichen Zahl f

$$\Delta(\mathfrak{O}) = \Delta(N) f^{-2} = (\sigma^2 - 4n) f^{-2},$$

und diese Zahl ist bekanntlich stets $\equiv 0$ oder $1 \bmod 4$.

Damit N der Bedingung (12a) genügt, darf $\mathfrak{O}$ keine Einheit $\neq \pm 1$ enthalten, d. h. es muß $\Delta(\mathfrak{O}) \neq -3, -4$ sein. Hiermit wird gleichzeitig auch $(A, B, C, D) \neq \sqrt{n}$ gewährleistet, was ja auch so geschrieben werden kann: $N \neq \sqrt{n}U$, $U \in \Gamma_0(q)$.

Die Anzahl $c^0_{n,0,0}$ der Klassen nach $\Gamma_0(q)$ konjugierter N der Eigenschaften (12), (12a) läßt sich hiernach folgendermaßen beschreiben: Man suche alle ganzen rationalen σ und f mit den Eigenschaften

$$(15) \qquad -2\sqrt{n} < \sigma < 2\sqrt{n},\ 0 < f,\ (\sigma^2 - 4n) f^{-2} \equiv 0 \text{ oder } 1 \bmod 4,\ (\sigma^2 - 4n) f^{-2} < -4.$$

Dann ist

$$(16) \qquad c^0_{n,0,0} = \sum_{\sigma, f} c\left((\sigma^2 - 4n) f^{-2}\right),$$

unter $c(\Delta)$ die Anzahl der Klassen nach $\Gamma_0(q)$ konjugierter in $\mathfrak{Q}$ optimal eingebetteter Ordnungen $U^{-1}\mathfrak{O}U$ mit der Diskriminante Δ verstanden. Diese Anzahl $c(\Delta)$ hängt nun eng mit der Idealklassenzahl der Ordnung $\mathfrak{O}$ der Diskriminante Δ zusammen [8]).

$\mathfrak{O}$ und $\mathfrak{O}_1$ seien in $\mathfrak{Q}$ optimal eingebettete Ordnungen derselben Diskriminante $\Delta < 0$. Sie sind also isomorph, und es gibt eine Matrix V so, daß $\mathfrak{O}_1 = V\mathfrak{O}V^{-1}$ ist. Hierdurch ist V bis auf den rechtsseitigen Faktor $W^\varepsilon M$ bestimmt, wo M dem durch $\mathfrak{O}$ erzeugten quadratischen Zahlkörper angehört und W ein Element ist, welches vermöge $\mathfrak{O} \to W\mathfrak{O}W^{-1}$ in $\mathfrak{O}$ den nicht identischen Automorphismus induziert; ε ist 0 oder 1. Wir schreiben daher $\mathfrak{O}_1 = (V_0 W^\varepsilon M)\, \mathfrak{O}\, (V_0 W^\varepsilon M)^{-1}$. Wegen dieser Gleichung ist $\mathfrak{O}$ auch in $\mathfrak{Q}_1 = (V_0 W^\varepsilon M)^{-1} \mathfrak{Q} (V_0 W^\varepsilon M)$ optimal eingebettet. Es gibt daher (s. oben, 6)) ein $\mathfrak{O}$-Ideal $\mathfrak{B}$ so, daß $\mathfrak{Q}_1$ die Rechtsordnung von $\mathfrak{Q}\mathfrak{B}$ ist. Da auch $\mathfrak{Q} V_0 W^\varepsilon M$ ein solches Ideal ist, gilt

$$\mathfrak{Q} V_0 W^\varepsilon M = \mathfrak{A}\mathfrak{B}$$

mit einem ambigen Ideal $\mathfrak{A}$. Man darf dieses ohne Beschränkung der Allgemeinheit in der Form $\mathfrak{A} = P_{p_1}^{e_1} P_{p_2}^{e_2} \ldots$, also als ganz und primitiv voraussetzen (s. oben, 3)). Ferner kann man $\mathfrak{B} = \mathfrak{B}_0 M'$ schreiben, wobei $\mathfrak{B}_0$ einem Repräsentantensystem der $\mathfrak{O}$-Idealklassen angehört; den Faktor M' kann man mit M auf der linken Seite vereinigen. Endlich zerlege man $\mathfrak{A}$ in ein Produkt $\mathfrak{A}_1 \mathfrak{A}_2$, wobei für die Primfaktoren p der Norm von $\mathfrak{A}_1$ die Gleichung $\left\{\frac{\Delta}{p}\right\} = 0$ gilt, für die Primfaktoren p der Norm von $\mathfrak{A}_2$ dagegen $\left\{\frac{\Delta}{p}\right\} \neq 0$ ist. Oben wurde unter 5) festgestellt, daß es ein $\mathfrak{O}$-Ideal $\mathfrak{B}'$ gibt, für das $\mathfrak{A}_1 = \mathfrak{Q}\mathfrak{B}'$ ist. Denkt man sich dieses mit $\mathfrak{B}$ vereinigt, so kommt man auf die Gleichung

$$(17) \qquad \mathfrak{Q} V_0 W^\varepsilon M = \mathfrak{A}_2 \mathfrak{B}_0.$$

Sie bringt zum Ausdruck, daß jeder mit $\mathfrak{O}$ isomorphen und zugleich mit $\mathfrak{O}$ in $\mathfrak{Q}$ optimal eingebetteten Ordnung $\mathfrak{O}_1$ zwei Paare (für $\varepsilon = 0$ und 1) $\mathfrak{A}_2$, $\mathfrak{B}_0$ eines ganzen primitiven ambigen $\mathfrak{O}$-Ideals und einer durch $\mathfrak{B}_0$ repräsentierten $\mathfrak{O}$-Idealklasse zugeordnet sind. Die beiden einem Paar $\mathfrak{O}, \mathfrak{O}_1$ zugeordneten Paare $\mathfrak{A}_2$, $\mathfrak{B}_0$ fallen dann und nur dann zu-

[8]) Die folgenden Überlegungen berühren sich engstens mit [3]), § 6.

sammen, wenn es eine Einheit der Form $E = WM$ in der Rechtsordnung $\mathfrak{O}_1$ von $\mathfrak{A}_2\mathfrak{B}_0$ gibt. Für $\mathfrak{A}_2$ gilt dabei $\left\{\frac{\Delta}{p}\right\} = 1$ für $p \mid n(\mathfrak{A}_2)$; die Anzahl dieser $\mathfrak{A}_2$ ist demnach gleich (13).

Diese Zuordnung ist auch eindeutig umkehrbar. Man gehe nämlich von einem ambigen $\mathfrak{O}$-Ideal $\mathfrak{A}_2$ der beschriebenen Art und einem Repräsentanten $\mathfrak{B}_0$ einer beliebigen $\mathfrak{O}$-Idealklasse aus. Das $\mathfrak{O}$-Linksideal $\mathfrak{A}_2\mathfrak{B}_0$ ist ein Hauptideal $\mathfrak{O}V$ (s. oben, 1)). $\mathfrak{O}$ ist dann in der Rechtsordnung von $\mathfrak{O}V$ optimal eingebettet (s. oben, 6)). Daher ist $\mathfrak{O}_1 = V\mathfrak{O}V^{-1}$ in $\mathfrak{O}$ optimal eingebettet. Nun ist aber V durch $\mathfrak{A}_2\mathfrak{B}_0$ nur bis auf eine Einheit E von $\mathfrak{O}$ als linksseitigen Faktor gegeben. Daher gehört zu dem Paar $\mathfrak{A}_2$, $\mathfrak{B}_0$ genau eine Klasse konjugierter Ordnungen $E\mathfrak{O}_1E^{-1}$.

Es kommt uns indessen auf die Klassen im engeren Sinne konjugierter Ordnungen $U\mathfrak{O}_1U^{-1}$ mit $U \in \Gamma_0(q)$, d. h. $|U| = +1$ an. $\Gamma_0(q)$ hat in der Einheitengruppe von $\mathfrak{O}$ den Index 2. Die Klassen $E\mathfrak{O}_1E^{-1}$ und $U\mathfrak{O}_1U^{-1}$ fallen dann und nur dann zusammen, wenn es eine Einheit E_1 mit $|E_1| = -1$, $E_1\mathfrak{O}_1E_1^{-1} = \mathfrak{O}_1$ gibt. Im anderen Falle zerfällt eine Klasse $E\mathfrak{O}_1E^{-1}$ in genau 2 Klassen $U\mathfrak{O}_1U^{-1}$. Eine solche Einheit muß von der Gestalt $E_1 = W_1^{\varepsilon}M_1$ sein, wobei W_1, M_1 dieselbe Bedeutung für $\mathfrak{O}_1$ haben wie oben W, M für $\mathfrak{O}$. Da $\Delta < 0$ ist, gilt $n(M_1) = |M_1| > 0$. Also kann nur $\varepsilon = 1$ sein. Ferner ist $W_1^2 = w$ eine rationale Zahl. Da w_1 und $\mathfrak{O}_2$ die ganze Matrixalgebra erzeugen, kann nicht $w < 0$ sein, denn sonst wäre diese Algebra zufolge $\Delta < 0$ definit. Folglich hat jede Einheit der Form $E_1 = W_1M_1$ die Norm (Determinante) -1. Es gibt somit ein solches E_1 dann und nur dann, wenn es ein $E = WM$ mit den obigen Eigenschaften in $\mathfrak{O}_1$ gibt. Infolge dieses Zusammentreffens ist

$$c(\Delta) = \prod_{p \mid q}\left(1 + \left\{\frac{\Delta}{p}\right\}\right) h(\Delta), \tag{18}$$

wo $h(\Delta)$ die Idealklassenzahl für die Ordnung $\mathfrak{O}$ mit der Diskriminante Δ bezeichnet.

Mit (16) und (18) ist die Anzahl $c_{n,0}^0$ unter Außerachtlassung derjenigen Koinzidenzpunkte berechnet worden, die in elliptischen Ecken liegen. Elliptische Ecken τ_0 gibt es nur von der Ordnung 2 oder 3. Ein Fixpunkt von N fällt in eine solche, wenn in (12a) das Gleichheitszeichen steht und $U^2 = -1$ oder $U^3 = \pm 1$ ist. Dieses U ist alsdann in der N zugeordneten Ordnung $\mathfrak{O}$ enthalten. Da hier andererseits $(\tau - \tau_0)^2$ bzw. $(\tau - \tau_0)^3$ als lokales Primelement gilt, muß das betreffende τ_0 bzw. N mit der Multiplizität $\frac{1}{2}$ bzw. $\frac{1}{3}$ gezählt werden. Nach wie vor bleibt indessen der Fall $N = \sqrt{n}U$, $U \in \Gamma_0(q)$ auszuschließen, der folgendermaßen beschrieben werden kann:

$$\sigma = 0, \Delta(0) = (\sigma^2 - 4n)f^{-2} = -4 \text{ bzw. } \sigma = \pm\sqrt{n},\ \Delta(0) = (\sigma^2 - 4n)f^{-2} = -3.$$

Das Endresultat kann man hiernach wie folgt zusammenfassen: Es bezeichnet $h(\Delta)$ und $w(\Delta)$ die Idealklassenanzahl und die halbe Einheitenanzahl der Ordnung mit der Diskriminante $\Delta < 0$. Dann ist die Gesamtmultiplizität der endlichen Koinzidenzpunkte

$$c_{n,0}^0 = \sum_{\sigma, f} \prod_{p \mid q}\left(1 + \left\{\frac{(\sigma^2 - 4n)f^{-2}}{p}\right\}\right) \frac{h((\sigma^2 - 4n)f^{-2})}{w((\sigma^2 - 4n)f^{-2})} - \gamma_{n,0} \tag{19}$$

$$(-2\sqrt{n} < \sigma < 2\sqrt{n},\ 0 < f,\ (\sigma^2 - 4n)f^{-2} \equiv 0 \text{ oder } 1 \bmod 4)$$

mit

$$\gamma_{n,0} = \begin{cases} 0 & \text{für } \sqrt{n} \not\equiv 0 \bmod 1, \\ \frac{1}{2}\prod_{p \mid q}\left(1 + \left(\frac{-4}{p}\right)\right) + \frac{2}{3}\prod_{p \mid q}\left(1 + \left(\frac{-3}{p}\right)\right) & \text{für } \sqrt{n} \equiv 0 \bmod 1. \end{cases} \tag{19a}$$

Wir haben also die zur Ausschließung von $N = \sqrt{n}U$, $U \in \Gamma_0(q)$ führende Summationsbeschränkung in (19) durch einen Korrekturterm kompensiert.

§ 3. Die Anzahl der unendlichen Koinzidenzpunkte.

Die rationalen Spitzen eines Fundamentalbereichs von $\Gamma_0(q)$ werden durch die $2^\varkappa$ Punkte $\tau = \infty, 0, q_1^{-1}$ vertreten, wo q_1 alle Teiler $\neq 1, q$ von q durchläuft. Wir ermitteln die Koinzidenzmultiplizitäten $c^0_{n,\mathfrak{p}_\tau}$ jedes einzelnen dieser Punkte.

Für $\tau = \infty$ ist $z_\infty = e^{2\pi i\tau}$ eine Ortsuniformisierende. Das gemäß § 1 zu bildende Ideal ist

$$\mathfrak{t}^0_{n,\mathfrak{p}_\infty} = \mathfrak{i}_{\mathfrak{p}_\infty} \prod_{r,s,t} \left(e^{2\pi i\tau} - e^{2\pi i\frac{s\tau+r}{t}}\right) = \mathfrak{i}_{\mathfrak{p}_\infty} \prod_{\substack{t\mid n\\ t\neq\sqrt{n}}} \left(z_\infty - z_\infty^{\frac{n}{t}}\right)\cdot\left(\frac{z_\infty^{\sqrt{n}} - w^{\sqrt{n}}}{z_\infty - w}\right)_{w=z_\infty}.$$

Das Produkt in der Mitte ist über ein System (7) von Zahlen r, s, t zu erstrecken; der letzte Faktor rechts fällt natürlich bei nicht quadratischem n fort. Der Grad von $\mathfrak{t}^0_{n,\mathfrak{p}_\infty}$ ist

$$c^0_{n,\mathfrak{p}_\infty} = 2\sum_{\substack{t\mid n\\ t<\sqrt{n}}} t + \begin{cases} 0 & \text{für } \sqrt{n} \not\equiv 0 \bmod 1,\\ \sqrt{n}-1 & \text{für } \sqrt{n} \equiv 0 \bmod 1.\end{cases} \tag{20}$$

Für $\tau = 0$ ist $z_0 = e^{-\frac{2\pi i}{q\tau}}$ ortsuniformierend. Man erkennt leicht, daß wegen $(n, q) = 1$ auch die Matrizen

$$\begin{pmatrix} s & 0\\ qr & t\end{pmatrix} \text{ mit } st = n,\ s > 0,\ 0 \leqq r < s, \text{ ausgenommen } s = t = \sqrt{n},\ r = 0$$

ein Vertretersystem derselben Klassen von bzgl. $\Gamma_0(q)$ linksseitig assoziierter Substitutionen der Determinante n bilden wie die Matrizen (7). Sie lassen den Punkt $\tau = 0$ fest. Die Koinzidenzmultiplizität berechnet sich demnach genau wie die von $\tau = \infty$:

$$c^0_{n,\mathfrak{p}_0} = c^0_{n,\mathfrak{p}_\infty}. \tag{21}$$

Endlich sei q_1 ein Teiler von q und $\mathfrak{p}_{q_1^{-1}}$ der zu $\tau = q_1^{-1}$ gehörige Punkt von K. Mit

$$L = \begin{pmatrix} 1 & 1\\ q_1 & q_1+1\end{pmatrix}, \qquad L^{-1} = \begin{pmatrix} q_1+1 & -1\\ -q_1 & 1\end{pmatrix}$$

und einer nicht weiter interessierenden rationalen Zahl r_1 ist $z_{q_1^{-1}} = e^{2\pi i r_1 L^{-1}(\tau)}$ hier ortsuniformisierend. Ist N eine q_1^{-1} fest lassende Substitution, so läßt $L^{-1}NL$ die Spitze ∞ fest. Kann man zeigen, daß die Matrizen

$$N = L\begin{pmatrix} s & r\\ 0 & t\end{pmatrix}L^{-1} = \begin{pmatrix} s + (s-r-t)\,q_1 & -s+r+t\\ (s-t)\,q_1 + (s-r-t)\,q_1^2 & t-(s-r-t)\,q_1\end{pmatrix} = \begin{pmatrix} A & B\\ qC & D\end{pmatrix} \tag{22}$$

mit $st = n$, $s > 0$, $r \bmod t$ reduziert, $(r, s, t) \neq \sqrt{n}$ ein Repräsentantensystem aller Klassen $\neq \sqrt{n}\,\Gamma_0(q)$ bzgl. $\Gamma_0(q)$ linksseitig assoziierter Substitutionen aus $\mathfrak{Q}$ der Determinante n bilden, so folgt auch für die Koinzidenzmultiplizität $c^0_{n,\mathfrak{p}_{q_1^{-1}}}$:

$$c^0_{n,\mathfrak{p}_{q_1^{-1}}} = c^0_{n,\mathfrak{p}_\infty}. \tag{23}$$

Daß dieses zutrifft, sieht man folgendermaßen ein. Aus (22) folgt

$$s = A + q_1 B,\ t = D - q_1 B,\ r = A - D + (1 + 2q_1)\,B \tag{24}$$

und

$$A - D = q_2 C - q_1 B \text{ mit } q_2 = \frac{q}{q_1}. \tag{25}$$

(25) ist notwendig und hinreichend für die Gültigkeit von (22). Es sei nun $\begin{pmatrix} a & b \\ qc & d \end{pmatrix}$ eine Substitution der Determinante n aus der Ordnung $\mathfrak{Q}$. Man suche ein $\begin{pmatrix} \alpha & \beta \\ q\gamma & \delta \end{pmatrix} \in \Gamma_0(q)$ so zu bestimmen, daß das Produkt

$$(26) \qquad \begin{pmatrix} \alpha & \beta \\ q\gamma & \delta \end{pmatrix}\begin{pmatrix} a & b \\ qc & d \end{pmatrix} = \begin{pmatrix} \alpha a + q\beta c & \alpha b + \beta d \\ q(\gamma a + \delta c) & q\gamma^b + \delta d \end{pmatrix} = \begin{pmatrix} A & B \\ qC & D \end{pmatrix}$$

die Gestalt (22) hat. Dazu muß also (25) gelten, was nach kurzer Umrechnung die Gestalt

$$(\alpha - q_2\gamma)(a + q_1 b) = (\delta - q_1\beta)(d + q_2 c)$$

annimmt. Diese Gleichung wird durch den Ansatz

$$(27) \qquad \alpha = v + q_2\gamma, \quad \delta = u + q_1\beta$$

gelöst, wobei u und v aus

$$(28) \qquad a + q_1 b = uh, \quad d + q_2 c = vh \quad \text{mit } h > 0 \text{ und } (u, v) = 1$$

zu entnehmen sind. Es muß aber noch

$$(29) \qquad 1 = \alpha\delta - q\beta\gamma = uv + vq_1\beta + uq_2\gamma$$

gelten. (29) ist ganzzahlig auflösbar, wenn $(uq_2, vq_1) = 1$ gilt, was man aus $ad - qbc = n$, $(n, q) = 1$ und (28) auch leicht entnimmt. Es ist also jedes $\begin{pmatrix} a & b \\ qc & d \end{pmatrix}$ mit einer Matrix (22) mod $\Gamma_0(q)$ linksseitig assoziiert.

In welchem Sinne liegen hierbei nun r, s, t fest? Aus (28) folgt: h ist der positiv genommene g. g. T. der Elemente in der ersten Spalte von $\begin{pmatrix} a & b \\ qc & d \end{pmatrix} L$. Wegen (26) ist h gleichzeitig der g. g. T. der Elemente in der ersten Spalte von $\begin{pmatrix} A & B \\ qC & D \end{pmatrix} L$, also auch wegen (22) von $L^{-1}\begin{pmatrix} A & B \\ qC & D \end{pmatrix} L$. D. h. es ist $h = s$. Aus (24) folgt weiter:

$$r = s - t + B,$$

aus (26), (27), (28):

$$r \equiv s - t + vb + \beta vh \bmod q_2,$$

aus (29):

$$r \equiv s - t + vb + \frac{1 - uv}{q_1} h \bmod q_2$$

und nochmals nach (28):

$$r \equiv s - t + \frac{h - av}{q_1} \equiv s - t + \frac{1}{q_1}\left(h - \frac{ad}{h}\right) \equiv s - t + \frac{1}{q_1}\left(h - \frac{n}{h}\right) \bmod q_2.$$

Das liefert wegen $h = s$:

$$r \equiv (1 + q_1^{-1})(s - t) \bmod q_2.$$

Die Restklasse von r mod q_2 ist also durch s, t festgelegt. Linksseitige Multiplikation von $\begin{pmatrix} A & B \\ qC & D \end{pmatrix}$ mit einer geeigneten Potenz von

$$L\begin{pmatrix} 1 & q_2 \\ 0 & 1 \end{pmatrix} L^{-1} = \begin{pmatrix} 1 - q & q_2 \\ -qq_1 & 1 + q \end{pmatrix} \in \Gamma_0(q)$$

erlaubt, r in ein vorgeschriebenes Repräsentantensystem der Restklassen mod tq_2 zu bringen. Dann gehört r einem, allerdings von $s - t$ abhängigen, Repräsentantensystem der Restklassen mod t an. Damit ist der Beweis von (23) fertig.

In Zusammenfassung des Erreichten geben wir jetzt die Spur des Heckeschen Operators T_n an. Nach (4) und (5) ist

$$T_n = T_n^0 + \begin{cases} 0 & \text{für } \sqrt{n} \not\equiv 0 \bmod 1, \\ T_1 & \text{für } \sqrt{n} \equiv 0 \bmod 1. \end{cases}$$

Die Spur von T_1 ist g, wie am Schluß von § 1 festgestellt wurde. Nach (8), (10), (11), (19), (19a), (20), (21), (23) (und $c^0_{n,\infty} = c^0_{n,\mathfrak{p}_\infty} + c^0_{n,\mathfrak{p}_0} + \Sigma\, c^0_{n,\mathfrak{p}_{q^{-1}}}$) ist

$$(30)\quad Sp(T_n) = \sum_{t|n} t - 2^\varkappa \sum_{\substack{t|n \\ t<\sqrt{n}}} -t \frac{1}{2} \sum_{\sigma,f} \prod_{p|q} \left(1 + \left\{\frac{(\sigma^2-4n)f^{-2}}{p}\right\}\right) \frac{h((\sigma^2-4n)f^{-2})}{w((\sigma^2-4n)f^{-2})} + \gamma_n$$

$$(-2\sqrt{n} < \sigma < 2\sqrt{n}, \quad 0 < f, \quad (\sigma^2-4n)f^{-2} \equiv 0 \text{ oder } 1 \bmod 4)$$

mit dem Korrekturterm

$$(30\text{a})\quad \gamma_n = \begin{cases} 0 & \text{für } \sqrt{n} \not\equiv 0 \bmod 1 \\ -2^{\varkappa-1}\sqrt{n} + g - 1 + \frac{1}{4}\prod_{p|q}\left(1 + \left(\frac{-4}{p}\right)\right) + \frac{1}{3}\prod_{p|q}\left(1 + \left(\frac{-3}{p}\right)\right) + 2^{\varkappa-1} & \text{für } \sqrt{n} \equiv 0 \bmod 1. \end{cases}$$

Dieser vereinfacht sich noch, wenn man die Formel

$$(31)\quad g = 1 - \frac{1}{4}\prod_{p|q}\left(1 + \left(\frac{-4}{p}\right)\right) - \frac{1}{3}\prod_{p|q}\left(1 + \left(\frac{-3}{p}\right)\right) - 2^{\varkappa-1} + \frac{1}{12}\prod_{p|q}(p+1)$$

für das Geschlecht von K heranzieht[9]). Hier ist $\varkappa$ die Anzahl der Primfaktoren von q.

§ 4. Die Darstellung der Multiplikatoren im Raume der Thetafunktionen.

Wie bisher bedeute q eine natürliche quadratfreie Zahl. In einer früheren Arbeit[3]) wurden Ideale der Stufe q in einer Quaternionen-Algebra Q eingeführt, die wir von jetzt ab als definit voraussetzen müssen. Es sei $\mathfrak{O}_1$ eine Ordnung der Stufe q in Q und $\mathfrak{M}_\nu$ ($\nu = 1, \ldots, H$) ein Vertretersystem der $\mathfrak{O}_1$-Linksidealklassen. Sind $\mathfrak{O}_\nu$ die Rechtsordnungen der $\mathfrak{M}_\nu$, so bilden $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu$ ein Vertretersystem aller $\mathfrak{O}_\mu$-Linksidealklassen. Durchläuft nun M alle Elemente $\neq 0$ aus $\mathfrak{M}_\nu^{-1}\mathfrak{M}_\mu$, so durchläuft $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu M$ alle ganzen mit $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu$ linksäquivalenten Ideale, und zwar jedes genau w_ν-mal, unter w_ν die Anzahl der Einheiten von $\mathfrak{O}_\nu$ verstanden. Aus den Anzahlen $\pi_{\mu\nu}(n)$ aller ganzen mit $\mathfrak{M}_\mu^{-1}\mathfrak{M}_\nu$ linksäquivalenten Ideale der Norm n wurde die H-reihige Anzahlmatrix

$$(32)\qquad P(n) = (\pi_{\mu\nu}(n))$$

gebildet.

Aus der eben gemachten Bemerkung geht hervor, daß $\pi_{\mu\nu}(n)\, w_\nu$ die Anzahl der $M \in \mathfrak{M}_\nu^{-1}\mathfrak{M}_\mu$ der Norm $n(M) = n \cdot n(\mathfrak{M}_\nu^{-1}\mathfrak{M}_\mu)$ ist. Bekanntlich sind die Thetareihen

$$\vartheta_{\mu\nu}(\tau) = \sum_{M \in \mathfrak{M}_\nu^{-1}\mathfrak{M}_\mu} e^{2\pi i \frac{n(M)}{n(\mathfrak{M}_\nu^{-1}\mathfrak{M}_\mu)}\tau} = 1 + \sum_{n=1}^{\infty} \pi_{\mu\nu}(n)\, w_\nu e^{2\pi i n\tau} = \left(\frac{1}{w_\nu} + \sum_{n=1}^{\infty} \pi_{\mu\nu}(n)\, e^{2\pi i n\tau}\right) w_\nu$$

ganze Modulformen (-2)-ten Grades zur Gruppe $\Gamma_0(q)$. Führt man noch die Matrix

$$P(0) = \begin{pmatrix} w_1^{-1} & \cdots & w_H^{-1} \\ \cdot & \cdots & \cdot \\ w_1^{-1} & \cdots & w_H^{-1} \end{pmatrix}$$

ein, so kann man die Gesamtheit dieser Thetareihen in Gestalt der Matrix

$$(33)\qquad \vartheta(\tau) = \sum_{n=0}^{\infty} P(n)\, e^{2\pi i n\tau}$$

schreiben.

[9]) S. [3]), S. 26.

Die Anwendung des Heckeschen Operators τ_p für eine nicht in q aufgehende Primzahl p ergibt nach § 1:

$$\vartheta(\tau) \mid \tau_p = \sum_{n=0}^{\infty} \sum_{r,s,t} P(n)\, e^{2\pi i n \frac{s\tau + r}{t}} \qquad (st = p,\ s > 0,\ 0 \leqq r < p)$$

$$= \sum_{n=0}^{\infty} \left(P(np) + pP\left(\frac{n}{p}\right) \right) e^{2\pi i n \tau},$$

wobei $P(r) = 0$ für ein gebrochenes r zu nehmen ist. Die rechte Seite ist nach früher angegebenen Formeln[10])

$$\vartheta(\tau) \mid \tau_p = P(p) \cdot \vartheta(\tau).$$

Da ferner die Anzahlmatrizen $P(n)$ und die Operatoren τ_n für $(n, q) = 1$ denselben Rechenregeln[10]) genügen, folgt aus der letzteren Gleichung allgemeiner

$$\vartheta(\tau) \mid \tau_n = P(n) \cdot \vartheta(\tau) \quad \text{für } (n, q) = 1. \tag{34}$$

Nach (34) erzeugen die $P(n)$ eine Darstellung des durch die τ_n mit $(n, q) = 1$ erzeugten Teilringes $\mathfrak{M}_1$ des ganzen Multiplikatorenringes $\mathfrak{M}$ von K. Die Spur dieser Darstellung ist bekannt und soll mit der Spur (30) von T_n verglichen werden. Vorher sind indessen noch drei Bemerkungen einzuschalten.

Erstens: Die Differenz je zweier Thetareihen zu quadratischen Formen des gleichen Geschlechts, also insbesondere von je zwei $\vartheta_{\mu\nu}(\tau)$, ist eine Spitzenform, wie man im Zuge des Beweises der Funktionalgleichung feststellt[11]). Die $P(n)$ erlauben daher einen einreihigen Bestandteil auszureduzieren; ihm entspricht diejenige Eisensteinreihe, welche nicht bereits zu einer kleineren Stufe gehört, nämlich

$$c_0 + \sum_{n=1}^{\infty} \sum_{\substack{t \mid n \\ (t,q)=1}} t e^{2\pi i n \tau}.$$

Der restliche $(H-1)$-reihige Bestandteil von $P(n)$ ist dann eine Darstellung von τ_n im Raume der durch Thetareihen erzeugbaren Spitzenformen, er werde aus einem gleich zu erläuternden Grunde mit $P_{q_1, q_2}(n)$ bezeichnet. Seine Spur ist für $(n, q) = 1$[12]):

$$Sp(P_{q_1, q_2}(n)) \tag{35}$$

$$= \frac{1}{2} \sum_{\sigma, f} \prod_{p \mid q_1} \left(1 - \left\{ \frac{(\sigma^2 - 4n) f^{-2}}{p} \right\} \right) \prod_{p \mid q_2} \left(1 + \left\{ \frac{(\sigma^2 - 4n) f^{-2}}{p} \right\} \right) \frac{h((\sigma^2 - 4n) f^{-2})}{w((\sigma^2 - 4n) f^{-2})} - \sum_{t \mid n} t + \gamma_n'$$

$$(-2\sqrt{n} < \sigma < 2\sqrt{n},\ 0 < f,\ (\sigma^2 - 4n) f^{-2} \equiv 0 \text{ oder } 1 \bmod 4)$$

mit

$$\gamma_n' = \begin{cases} 0 & \text{für } \sqrt{n} \not\equiv 0 \bmod 1, \\ \dfrac{1}{12} \prod\limits_{p \mid q_1} (p-1) \prod\limits_{p \mid q_2} (p+1) & \text{für } \sqrt{n} \equiv 0 \bmod 1. \end{cases} \tag{35a}$$

Zweitens: In (35) ist $q = q_1 q_2$ eine Zerlegung von q, wobei q_1^2 die Diskriminante der Algebra Q ist. Der Faktor q_1 ist stets das Produkt einer ungeraden Anzahl von Primfaktoren, nämlich der endlichen Verzweigungsstellen der Algebra Q, während q_2 keiner

---

[10]) Vgl. [3]), Formeln (24) und (25).

[11]) S. etwa *M. Eichler*, Quadratische Formen und orthogonale Gruppen, Berlin-Göttingen-Heidelberg 1952, S. 141–142.

[12]) Formel (63) (und (18)) in [3]).

Beschränkung unterliegt. Drittens sind Modulformen zur Gruppe $\Gamma_0(q')$ für einen Teiler q' von q auch Modulformen zu $\Gamma_0(q)$. Man wird Thetareihen zu verschiedenen Teilern q' heranziehen und die entsprechenden Darstellungen $P_{q'_1, q'_2}(n)$ addieren müssen, wenn man einen Vergleich von ihnen mit T_n im Auge hat.

Als ersten Fall behandeln wir nun den einer Primzahlstufe $q = p$. Die Spuren (30) und (35) stimmen überein:

$$(36) \qquad Sp(P_p(n)) = Sp(T_n) \qquad \text{für } (n, p) = 1,$$

falls das folgende zutrifft:

$$(37) \qquad \sum_{\sigma, f} \frac{h((\sigma^2 - 4n) f^{-2})}{w((\sigma^2 - 4n) f^{-2})} = 2 \sum_{\substack{t \mid n \\ t > \sqrt{n}}} t + \begin{cases} 0 & \text{für } \sqrt{n} \not\equiv 0 \bmod 1, \\ \sqrt{n} + \dfrac{1}{6} & \text{für } \sqrt{n} \equiv 0 \bmod 1; \end{cases}$$

dabei ist von (31) Gebrauch gemacht worden. (37) ist aber die bekannte Klassenzahlrelation der 1. Stufe[13]). Man erhält einen neuen Beweis von (37) im gleichen Zuge, wenn man $p = 2$ wählt. Dann ist $g = 0$, $H = 1$, und beide Seiten von (36) sind 0. Wir ziehen aus (36) die Schlußfolgerung:

Satz 1. *Im Falle einer Primzahlstufe q lassen sich alle ganzen Modulformen (-2)-ten Grades zu $\Gamma_0(q)$ durch Thetareihen zu quaternären quadratischen Formen der Stufe q (Diskriminante q^2) linear kombinieren.*

Beweis. Nach (36) erfährt der durch die τ_n mit $(n, q) = 1$ erzeugte Unterring $\mathfrak{M}_1$ des Multiplikatorenringes $\mathfrak{M}$ von K im Raume der Spitzenformen sowie in dem durch Thetareihen erzeugten Teilraume äquivalente Darstellungen. Daher sind diese Räume linear äquivalent, d. h. sie haben die gleichen Dimension. Folglich gibt es zu jeder Spitzenform $\sigma(\tau)$ eine Linearkombination $\lambda(\tau)$ von Thetareihen derart, daß die $q - 1$ ersten Entwicklungskoeffizienten der Differenz $\sigma(\tau) - \lambda(\tau)$ für die Spitze $\tau = \infty$ verschwinden. Nach einem Satze von Hecke ist dann identisch $\sigma(\tau) - \lambda(\tau) = 0$. Auch die einzige Eisensteinreihe kann bekanntlich durch Thetareihen dargestellt werden.

Nunmehr folgt übrigens (36) auch für $(n, q) > 1$, wenn man für T_n den von Hecke mit T_n^q bezeichneten Operator nimmt.

Hierauf wollen wir nur noch die Fälle behandeln, wo q das Produkt von 2 oder 3 Primzahlen ist:

$$(38) \qquad Sp(P_{p_1, p_2}(n) + 2P_{p_1, 1}(n)) = Sp(T_n) \quad \text{für } q = p_1 p_2,\ (n, q) = 1,$$

$$(39) \qquad \begin{aligned} Sp(P_{p_1 p_2 p_3, 1}(n) + \sum_{i \neq k} P_{p_i, p_k}(n)) &= Sp(P_{p_1, p_2 p_3}(n) + 2P_{p_1, p_2}(n) + 4P_{p_1, 1}(n)) \\ &= Sp(T_n) \quad \text{für } q = p_1 p_2 p_3,\ (n, q) = 1. \end{aligned}$$

Beide Formeln ergeben sich wie (36) aus dem Vergleich von (30) und (35), unter Berücksichtigung der Formel (31) für das Geschlecht sowie der Klassenzahlrelation (37) der 1. Stufe. Die Satz 1 entsprechende Schlußfolgerung lautet:

Satz 2. *Streicht man in den ganzen Modulformen $\varphi(\tau) = \sum_n a(n) e^{2\pi i n \tau}$ alle Reihenglieder mit $(n, q) > 1$, so lassen sich die entstehenden Reihen durch in gleicher Weise abgeänderte Thetareihen von Stufen $q' \mid q$ linear kombinieren, wenn q ein Produkt von höchstens 3 Primfaktoren ist.*

---

[13]) *F. Klein* und *R. Fricke*, Vorlesungen über die Theorie der elliptischen Modulfunktionen, Teil II, Leipzig 1892, S. 184.

q sei ein Produkt von 2 oder 3 Primfaktoren, von denen mindestens einer $= 11$ oder > 13 ist. Dann enthält die Darstellung des durch die τ_n mit $(n, q) = 1$ erzeugten Teilringes $\mathfrak{M}_1$ des Multiplikatorenringes im Raume der Differentiale 1. Gattung mindestens einen Bestandteil mehrfach. Es gibt Spitzenformen (-2)-ten Grades, welche sich nicht durch Thetareihen einer Stufe $q' \mid q$ darstellen lassen.

Beweis. Der erste Teil ergibt sich genau wie Satz 1 aus (38) bzw. (39). Die rechte Seite von (38) hängt nur von dem Produkt $q = p_1 p_2$ ab. Man darf daher links p_1 und p_2 vertauschen und folglich $p_2 = 11$ oder > 13 annehmen. Dann ist $P_{p_2, 1}(n)$ eine mindestens einreihige Darstellung, welche laut (38) in der Darstellung T_n mindestens zweimal vorkommt. Analog kann im Falle (39) geschlossen werden. Hiernach gibt es weniger linear unabhängige durch Differenzen von Thetareihen zu Quaternionen-Idealen des „Typus" (p_1, p_2) und $(p_2, 1)$ bzw. $(p_1, p_2 p_3)$ und (p_2, p_3) und $(p_3, 1)$ darstellbare Spitzenformen als linear unabhängige Spitzenformen überhaupt. Die Gesamtheit der durch die genannten speziellen Thetareihen dargestellten Spitzenformen stimmt nun aber mit der Gesamtheit aller durch Thetareihen einer Stufe $q' \mid q$ erzeugbaren Spitzenformen überein, wie aus den Formeln

$$Sp(P_{p_1, p_2}(n) + 2P_{p_2, 1}(n)) = Sp(P_{p_2, p_1}(n) + 2P_{p_1, 1}(n)),$$

$$Sp(P_{p_1 p_2 p_3, 1}(n) + \sum_{i \neq k} P_{p_i, p_k}(n)) = Sp(P_{p_i, p_j p_k}(n) + 2P_{p_j, p_k}(n) + 4P_{p_k, 1}(n)) \quad (i \neq j \neq k \neq i)$$

hervorgeht, welche unmittelbar aus den a. a. O.[12]) angegebenen Formeln folgen, und zwar auch für $(n, q) > 1$. Das liefert die letzte Behauptung von Satz 2.

§ 5. Bemerkungen zu den Klassenzahlrelationen.

Die Mehrzahl der bekannten Klassenzahlrelationen, wenn nicht überhaupt alle, beruhen im Prinzip darauf, daß man die Spur (30) von T_n durch die n-ten Entwicklungskoeffizienten von Spitzenformen (-2)-ten Grades ausdrückt. Daß dieses möglich ist, ergibt sich als eine auf der Hand liegende Folgerung aus der Heckeschen Theorie. Die Auswertung durch mehr oder minder elementare zahlentheoretische Funktionen gelingt natürlich nur für kleine Stufen. Die Erkenntnis über diese allgemeine Natur der Klassenzahlrelationen hat aber auch davon abgesehen einigen Wert. Man verdankt sie Hurwitz[14]), auf den im Prinzip alle von uns hier verwendeten Schlüsse zurückgehen. Dazu gehört insbesondere auch der Grundgedanke der Heckeschen Theorie, der sich bei Hurwitz allerdings nicht auf die den Differentialen 1. Gattung entsprechenden Modulformen, sondern auf die Integrale 1. Gattung stützt. Das von ihm erst ein Jahr später aufgestellte Spurtheorem, unsere Formel (8), wird in kunstvoller Weise umgangen, jedoch so, daß man vermuten könnte, daß gerade die hierzu notwendigen Überlegungen wenig später zu diesem allgemeinen Theorem führten.

Bei der erwähnten Schwierigkeit, die „anderen Seiten" der Klassenzahlrelationen explizit auszuwerten, könnte man die Frage stellen, ob man nicht durch Kombination verschiedener solcher Relationen einfach berechenbare andere Seiten erhält. Von der Seite der Funktionentheorie her scheint die Frage hoffnungslos schwierig zu sein. Daß es aber in der Tat möglich ist, zeigt das arithmetische Gegenstück zu dieser Arbeit[3]).

Bisher war verschwiegen worden, daß Hurwitz nicht bei $\Gamma_0(q)$ invariante Funktionen benutzt, sondern die Modulfunktionen zu der Hauptkongruenzuntergruppe $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

[14]) *A. Hurwitz*, Über die Klassenzahlrelationen und Modularkorrespondenzen primzahliger Stufe, Berichte d. k. sächsischen Ges. d. Wiss. Leipzig Math.-Phys. Kl. 37 (1885), S. 222–240 = Math. Werke II, Basel 1933, S. 51–67.

mod q. Er kommt so zu gewissermaßen feineren Klassenzahlrelationen. Es wäre möglich und interessant, die entsprechenden Verfeinerungen auch in der Arithmetik der Quaternionen-Algebren durchzuführen.

§ 6. Die Darstellbarkeit von Modulformen geraden Grades durch Thetareihen.

Von jetzt ab wird vorausgesetzt, daß die Stufe q eine Primzahl ist, so daß Satz 1 herangezogen werden kann. Zunächst beweisen wir den

Hilfssatz. *Wenn q hinreichend groß ist, gibt es eine Spitzenform $\sigma(\tau) = \Sigma\, s(n)\, e^{2\pi i n \tau}$ (-2)-ten Grades zu $\Gamma_0(q)$ mit $s(1) = 0$, $s(2) \neq 0$, $s(q) \neq 0$.*

Zum Beweise ziehen wir die Anzahlmatrizen $P(n)$ zu der Quaternionen-Algebra Q der Diskriminante q^2 heran. Und zwar legen wir eine solche Anordnung der Idealklassen zugrunde, daß die Rechtsordnungen der ersten t_1 Klassenrepräsentanten $\mathfrak{M}_\nu$ ambige Hauptideale der Norm q besitzen, während für die Rechtsordnungen der übrigen $\mathfrak{M}_\nu$ die ambigen Ideale der Norm q nicht Hauptideale sind. Diese letzteren treten dann je zweimal auf; man kann daher die Anordnung so treffen, daß die Rechtsordnungen von $\mathfrak{M}_{t_1+\nu}$ und $\mathfrak{M}_{t_1+t_2+\nu}$ $(\nu = 1, \ldots, t_2)$ gleich (bzw. isomorph) sind. Die Anzahlmatrix läßt sich dann so unterteilen:

$$P(n) = \begin{pmatrix} U_1 & V & V \\ \dot{V} & U_2 & \widetilde{U}_2 \\ \dot{V} & \dot{\widetilde{U}}_2 & U_2 \end{pmatrix}. \tag{40}$$

Die Spaltenanzahlen von U_1 und V sind t_1 und t_2; gleich bezeichnete Teilmatrizen sind gleich. Die Klassenanzahl ist $H = t_1 + 2t_2$, die Typenanzahl $T = t_1 + t_2$. Aus den Formeln für diese Anzahlen[15]) geht hervor, daß sie mit q unbegrenzt wachsen, ebenso wie auch ihre Differenz t_2.

Vorweg sei bemerkt, daß nach der Spurformel $0 \leqq Sp(P(2)) \leqq 4$ ist; ferner ist die Summe jeder Zeile von $P(2)$ gleich 3.

Dem Schema (40) entspricht gleichzeitig eine Anordnung der quadratischen Formen $Q_\nu(x)$ der Diskriminante q^2. Die Anzahl $a_\nu(n)$ der Darstellungen von n durch $Q_\nu(x)$ ist nach § 4 im wesentlichen gleich dem entsprechenden Koeffizienten von $P(n)$. Die Zahl 1 wird nur von den in der Hauptdiagonale von U_1 und U_2 stehenden Formen dargestellt, die Zahl q nur von den in der Hauptdiagonalen von U_1, $\widetilde{U}_2$, $\dot{\widetilde{U}}_2$.

Nach diesen Vorbereitungen wählen wir drei Formen $Q_\nu(x)$, $\nu = 0, 1, 2$. Und zwar liege $Q_0(x)$ in U_1, aber nicht auf der Hauptdiagonalen, und stelle die 2 nicht dar. Ein solches $Q_0(x)$ gibt es, wenn $t_1 > 4$ ist. $Q_1(x)$ liege in U_1 oder V, aber ebenfalls nicht auf der Hauptdiagonalen, und stelle die 2 dar. $Q_2(x)$ auf der Hauptdiagonalen von $\widetilde{U}_2$; dazu muß also $t_2 > 0$ vorausgesetzt werden. Über die Darstellungsanzahlen $a_\nu(n)$ kann man dann das folgende in Form einer Tabelle aussagen:

	$n = 0$	1	2	q
$\nu = 0$	1	0	0	0
1	1	0	> 0	0
2	1	0	$\geqq 0$	> 0

[15]) Satz 11 in 3).

Bei geeigneter Bestimmung des Koeffizienten c ist

$$\sigma(\tau) = \sum_{(x)} \left(e^{2\pi i Q_s(x)\tau} - e^{2\pi i Q_s(x)\tau} + c\left(e^{2\pi i Q_1(x)\tau} - e^{2\pi i Q_s(x)\tau}\right)\right)$$

eine Spitzenform der im Hilfssatz verlangten Beschaffenheit.

Das Differential 1. Gattung $du = \frac{1}{2\pi i}\,\sigma(\tau)\,d\tau$ verhält sich in der Spitze $\tau = \infty$ des Fundamentalbereichs mit der Ortsuniformisierenden $z_\infty = e^{2\pi i\tau}$ folgendermaßen:

$$du = (s(2)\,z_\infty + s(3)\,z_\infty^2 + \cdots)\,dz_\infty, \quad s(2) \neq 0.$$

Die andere Spitze des Fundamentalbereichs ist $\tau = 0$ mit der Ortsuniformisierenden $z_0 = e^{-\frac{2\pi i}{q\tau}}$. Die Entwicklung von $\sigma(\tau)$ an dieser Stelle erhält man durch Anwendung der Fundamentalgleichung der Thetafunktionen:

$$\sigma(\tau) = \frac{-1}{q\tau^2} \sum_{(x)} \left(e^{-\frac{2\pi i}{q\tau}\tilde{Q}_s(x)} - e^{-\frac{2\pi i}{q\tau}\tilde{Q}_s(x)} + c\left(e^{-\frac{2\pi i}{q\tau}\tilde{Q}_1(x)} - e^{-\frac{2\pi i}{q\tau}\tilde{Q}_s(x)}\right)\right),$$

wobei $\tilde{Q}_\nu(x)$ die primitiven Adjungierten zu $Q_\nu(x)$ sind. Für ihre Darstellungsanzahlen gilt bekanntlich $\tilde{a}_\nu(n) = a_\nu(qn)$. Nach dem Hilfssatz ist daher

$$du = -\left(s(q) + s(2q)\,z_0 + \cdots\right)dz_0, \quad s(q) \neq 0.$$

Hiernach ist du ein Differential 1. Gattung, welches in $\tau = \infty$ eine einfache Nullstelle hat und in $\tau = 0$ nicht verschwindet. Da der Körper K der Modulfunktionen zu $\Gamma_0(q)$ den Automorphismus

$$(41) \qquad \alpha: \ \tau \to \frac{-1}{q\tau}, \quad \text{d. h.} \quad \varphi(\tau)^\alpha = \varphi\left(\frac{-1}{q\tau}\right)$$

besitzt, hat das Differential du^α in $\tau = 0$ eine einfache Nullstelle und verschwindet nicht in $\tau = \infty$. Damit sind die Vorbereitungen für den folgenden Satz beendet:

Satz 3. *Für eine hinreichend große Primzahlstufe q lassen sich alle ganzen Modulformen $(-2k)$-ten Grades $(k = 1, 2, \ldots)$ zu $\Gamma_0(q)$ durch $4k$-fache Thetareihen zu den Stufen* 1 *und q linear kombinieren.*

Beweis. Der Fall $k = 1$ wurde bereits mit Satz 1 erledigt. Für $k = 2$ gibt es eine Thetareihe der Stufe 1, nämlich zu der definiten Form in 8 Variablen mit der Diskriminante 1. Sie stimmt bekanntlich mit der Eisensteinreihe überein. Wir bezeichnen sie mit $E(\tau)$. Es sei $Q(x)$ irgendeine definite quaternäre Form der Diskriminante q^2 und $\vartheta(\tau)$ die zugehörige Thetareihe. Die ersten Terme in den Reihenentwicklungen von $E(\tau)$ und $\vartheta^2(\tau)$ an den Stellen $\tau = \infty$ und $\tau = 0$ sind dann

$$E(\tau) = 1 + \cdots = \tau^{-4}(1 + \cdots), \quad \vartheta^2(\tau) = 1 + \cdots = \tau^{-4}(q^{-2} + \cdots).$$

Man kann daher jede Modulform des Grades -4 durch Addition einer passenden Linearverbindung von $E(\tau)$ und $\vartheta^2(\tau)$ zu einer Spitzenform machen. Bei Modulformen des Grades $-2k\,(k > 2)$ gelingt dasselbe unter Benutzung von $E(\tau)\,\vartheta^{k-2}(\tau)$ und $\vartheta^k(\tau)$. Es genügt daher, Satz 3 für Spitzenformen zu beweisen.

Ist $\varphi(\tau)$ eine Spitzenform des Grades $-2k$, so ist $\varphi(\tau)\,d\tau^k$ ein Differential k-ten Grades, d. h. der ihm zugeordnete Divisor gehört der k-ten Potenz der Differentialklasse an. Dieser Divisor ist ganz bis auf Pole höchstens $(k-1)$-ter Ordnung in den Punkten $\tau = \infty, 0$. Durch Addition einer passenden Linearkombination von $du(\vartheta(\tau)\,d\tau)^{k-1}$ und $du^\alpha(\vartheta(\tau)\,d\tau)^{k-1}$, wo du und du^α die oben konstruierten ganzen Differentiale sind, kann

man die Polordnungen von $\varphi(\tau)\,d\tau^k$ auf $\leqq k-2$ herabdrücken. Darauf addiert man eine geeignete Linearkombination von $du^2(\vartheta(\tau)\,d\tau)^{k-2}$, $dudu^\alpha(\vartheta(\tau)\,d\tau)^{k-2}$, $(du^\alpha)^2(\vartheta(\tau)\,d\tau)^{k-2}$ und fährt so fort, bis man zu einem überall ganzen Differential k-ten Grades kommt. Man beachte dabei, daß alle benutzten Differentiale $du(\vartheta(\tau)\,d\tau)^{k-1}$ usw. ihrer Konstruktion gemäß (bis auf den Faktor $d\tau^k$) durch Produkte von k quaternären Thetareihen, d. h. durch $4k$-fache Thetareihen darstellbar sind.

Ein überall ganzes Differential $\varphi(\tau)\,d\tau^k$ des Grades k ist nun nach einem Satz von M. Noether [16]) als ein homogenes Polynom k-ten Grades in den Differentialen 1. Gattung darstellbar, sofern der Körper K nicht (elliptisch oder) hyperelliptisch ist. Die Differentiale 1. Gattung sind aber nach Satz 1 durch vierfache Thetareihen darstellbar, und es folgt Satz 3.

Es bleibt zum Schluß übrig zu zeigen, daß der Körper K für genügend großes q nicht hyperelliptisch ist. K ist Erweiterung 2. Grades des bei dem Automorphismus (41) elementweise invarianten Unterkörpers K_1. Das Geschlecht von K_1 ergibt sich unter Voraussetzung von Satz 1 als $g_1 = t_2$, d. h. als die Reihenanzahl der Teilmatrix U_2 in (40) [17]).

Wir nehmen jetzt im Gegensatz zur Behauptung an, K besitze eine Erzeugung $K = k(x, \sqrt{f(x)})$ mit einem quadratfreien Polynom $f(x)$. Es seien dw_i die Differentiale 1. Gattung, speziell $dw_0 = f(x)^{-\frac{1}{2}}\,dx$. Dann sind die Quotienten $\dfrac{dw_i}{dw_0}$ insgesamt g linear unabhängige Polynome höchstens $(g-1)$-ten Grades in x. Andererseits bezeichnen wir die Differentiale 1. Gattung von K mit du_i $(i = 1, \ldots, g_1)$, dv_i $(i = 1, \ldots, g - g_1)$ und setzen voraus: $du_i^\alpha = du_i$, $dv_i^\alpha = -dv_i$. Ist $t_1 > 0$, $t_2 > 0$, so kommen Differentiale beider Sorten vor. Der Unterkörper $k(x)$ wird durch die Quotienten der Differentiale 1. Gattung erzeugt; folglich induziert auch α in $k(x)$ den nicht identischen Automorphismus. Dieser hat dann bekanntlich die folgende Gestalt:

$$x^\alpha = \frac{ax+b}{cx+d} \quad \text{mit } ad - bc \neq 0 \text{ und, wegen } \alpha^2 = 1,\ a + d = 0.$$

Nach geeigneter gebrochen linearer Transformation von x darf man ohne Beschränkung der Allgemeinheit $x^\alpha = -x$ annehmen. Jetzt geht $dw_0 = f(x)^{-\frac{1}{2}}\,dx$ bei α in $\pm\, dw_0$ über, also ist dw_0 entweder ein du oder ein dv. Folglich gibt es g_1 bzw. $g - g_1$ linear unabhängige Quotienten $\dfrac{dw_i}{dw_0}$, die bei α invariant sind bzw. das Vorzeichen wechseln. Die ersteren müßten Polynome in x^2, die letzteren x mal Polynome in x^2 sein. Demnach dürften sich ihre Anzahlen höchstens um 1 unterscheiden:

$$|\, g_1 - (g - g_1)\,| = |\, g - 2g_1\,| = |\, t_1 - 1\,| \leqq 1.$$

Diese Ungleichung trifft aber nicht zu, wenn $t_1 > 1$ ist, und das ist für fast alle q der Fall.

---

[16]) *K. Hensel* und *G. Landsberg*, Theorie der algebraischen Funktionen einer Variablen, Leipzig 1902, S. 502.

[17]) *M. Deuring*, Die Anzahl der Typen von Maximalordnungen ..., J.-ber. Deutsche Math. Vereing. **54** (1944/45), S. 24–54, bes. S. 31. Auf ganz anderem Wege bestimmte *R. Fricke* dieses Geschlecht: Die elliptischen Funktionen und ihre Anwendungen, Teil II, Leipzig 1922, S. 363 und 366.

Eingegangen 5. Oktober 1954.

Bemerkungen zur additiven Zahlentheorie. III.

Vereinfachter Beweis eines Satzes von A. Brauer.

Von *Alfred Stöhr* in Göttingen.

$\mathfrak{A}$ und $\mathfrak{B}$ seien Mengen nichtnegativer ganzer Zahlen. $\mathfrak{A}$ habe die Dichte α mit $0 < \alpha < 1$. Es sei $0 \in \mathfrak{B}$, $1 \in \mathfrak{B}$. Für jede natürliche Zahl m sei $l(m)$ gleich der kleinsten Zahl l, für die

$$m = b_1 + \cdots + b_l \tag{1}$$

in Zahlen $b_1, \ldots, b_l$ aus $\mathfrak{B}$ lösbar ist. Es werde

$$\overline{\operatorname{fin}}_{n=1,2,\ldots} \frac{1}{n} \sum_{m=1}^{n} l(m) = \lambda$$

gesetzt; dabei sei $\lambda < \infty$. Die Summe der Mengen $\mathfrak{A}$ und $\mathfrak{B}$ werde mit $\mathfrak{C}$ bezeichnet; wegen $0 \in \mathfrak{B}$ ist $\mathfrak{A} \subseteq \mathfrak{C}$. Mit $A(n)$ bzw. $C(n)$ bezeichnen wir für natürliches n die Anzahl der positiven Zahlen $\leqq n$ aus $\mathfrak{A}$ bzw. aus $\mathfrak{C}$. Dann gilt[1])

$$\frac{C(n)}{n} > \alpha\left(1 + \frac{1-\sqrt{\alpha}}{\lambda}\right), \tag{2}$$

also, wenn γ die Dichte von $\mathfrak{C}$ ist,

$$\gamma \geqq \alpha\left(1 + \frac{1-\sqrt{\alpha}}{\lambda}\right).$$

Der folgende Beweis benutzt die Grundgedanken der Beweise von A. Brauer und seiner Vorgänger Erdös und Landau; die einzige hier neue Wendung, die in diesem Beweisgang eine Abkürzung ergibt, wird durch Kursivschrift hervorgehoben.

Für festes natürliches n und $1 \leqq m \leqq n$ sei $D(m)$ die Anzahl der Zahlen $a \in \mathfrak{A}$ mit

$$1 \leqq a < a + m \leqq n \quad \text{und} \quad a + m \notin \mathfrak{A}; \tag{3}$$

ferner sei $E(m)$ die Anzahl der Zahlen $a \in \mathfrak{A}$ mit $1 \leqq a < a + m \leqq n$ und $a + m \in \mathfrak{A}$. Dann ist $D(m) = A(n-m) - E(m)$ und, wenn k eine ganze Zahl mit $0 \leqq k \leqq n$ ist,

$$\sum_{m=1}^{k} D(m) = \sum_{m=1}^{k} A(n-m) - \sum_{m=1}^{k} E(m) \geqq \sum_{m=1}^{k} A(n-m) - \sum_{m=1}^{n} E(m).$$

Die letzte Summe über $E(m)$ ist gleich der Anzahl der Zahlenpaare $a, a' \in \mathfrak{A}$ mit $1 \leqq a < a' \leqq n$, also gleich $\frac{1}{2} A^2(n) - \frac{1}{2} A(n)$. Das liefert

---

[1]) *A. Brauer*, Über die Dichte der Summe zweier Mengen, deren eine von positiver Dichte ist, Math. Zeitschr. 44, 212—232 (1939).

$$\sum_{m=1}^{k} D(m) \geqq \sum_{m=1}^{k} A(n-m) + \frac{1}{2} A(n) - \frac{1}{2} A^2(n)$$

$$\geqq \sum_{m=1}^{k} \alpha(n-m) + \frac{1}{2} \alpha n - \frac{1}{2} A^2(n)$$

$$= \frac{\alpha}{2} \{(2n-k)k + n - k\} - \frac{1}{2} A^2(n).$$

Wählt man zu m eine feste Zerlegung (1) und bestimmt für jedes der in der Anzahl $D(m)$ vorhandenen $a \in \mathfrak{A}$ mit (3) den kleinsten Index j, für den $a + b_1 + \cdots + b_{j-1} \in \mathfrak{A}$, aber $r = a + b_1 + \cdots + b_j \notin \mathfrak{A}$ ist, so ist

$$(4) \qquad 1 \leqq r \leqq n, \quad r \in \mathfrak{C}, \quad \text{aber} \quad r \notin \mathfrak{A}.$$

Die r mit der Eigenschaft (4) sind genau in der Anzahl $C(n) - A(n)$ vorhanden, und für den Index j kommen die Werte $1, 2, \ldots, l(m)$ in Betracht. Also ist

$$D(m) \leqq l(m)\,(C(n) - A(n)).$$

Summation ergibt

$$\sum_{m=1}^{k} D(m) \leqq \sum_{m=1}^{k} l(m)\,(C(n) - A(n)) \leqq \lambda k (C(n) - A(n)),$$

also

$$(5) \qquad \lambda k (C(n) - A(n)) \geqq \frac{\alpha}{2} \{(2n-k)k + n - k\} - \frac{1}{2} A^2(n).$$

z sei eine nicht notwendig ganze Zahl mit $0 < z < n$, über die wir noch verfügen werden. Wir definieren η und ϑ durch $[z] = z - \eta$, $[z] + 1 = z + \vartheta$; es ist also $0 \leqq z - \eta < z + \vartheta \leqq n$, $\eta \geqq 0$, $\vartheta > 0$, $\eta + \vartheta = 1$. Mit $k = z - \eta$ liefert (5)

$$(6) \quad \lambda(z-\eta)\,(C(n) - A(n)) \geqq \frac{\alpha}{2} \{(2n - z + \eta)(z - \eta) + n - z + \eta\} - \frac{1}{2} A^2(n).$$

Mit $k = z + \vartheta$ *liefert* (5)

$$(7) \quad \lambda(z+\vartheta)\,(C(n) - A(n)) \geqq \frac{\alpha}{2} \{(2n - z - \vartheta)(z + \vartheta) + n - z - \vartheta\} - \frac{1}{2} A^2(n).$$

Wir multiplizieren die Ungleichung (6) *mit* ϑ *und die Ungleichung* (7) *mit* η *und addieren; wegen* $\eta + \vartheta = 1$ *ergibt das*

$$\lambda z (C(n) - A(n)) \geqq \frac{\alpha}{2} \{(2n - z)z + n - z - \eta\vartheta\} - \frac{1}{2} A^2(n).$$

Wegen $n - z - \eta\vartheta > n - (z + \vartheta) \geqq 0$ *folgt*

$$(8) \qquad \lambda z (C(n) - A(n)) > \frac{\alpha}{2}(2n - z)z - \frac{1}{2} A^2(n),$$

$$\frac{C(n)}{n} > \frac{A(n)}{n} + \frac{1}{\lambda z n} \left\{ \frac{\alpha}{2}(2n - z)z - \frac{1}{2} A^2(n) \right\}.$$

Wählen wir hier $z = \sqrt{\alpha}\, n$ (man kann sich überlegen, daß dieser Wert das optimale Endergebnis liefert), so haben wir

$$\frac{C(n)}{n} > \frac{A(n)}{n} + \frac{\alpha}{2\lambda}(2 - \sqrt{\alpha}) - \frac{1}{2\lambda\sqrt{\alpha}} \left(\frac{A(n)}{n}\right)^2 ;$$

außerdem gilt die triviale Abschätzung $\frac{C(n)}{n} \geqq \frac{A(n)}{n}$. Da $\frac{A(n)}{n} \geqq \alpha$ ist und da die Funktion

$$h(\xi) = \max\left(\xi, \xi + \frac{\alpha}{2\lambda}(2-\sqrt{\alpha}) - \frac{1}{2\lambda\sqrt{\alpha}}\xi^2\right)$$

für $\xi < \alpha$ der Ungleichung $h(\xi) > h(\alpha)$ genügt [2]), folgt

$$\frac{C(n)}{n} > h(\alpha) = \alpha\left(1 + \frac{1-\sqrt{\alpha}}{\lambda}\right).$$

Damit ist (2) bewiesen.

Anmerkung. A. Brauer gewinnt (8) aus

$$\lambda z(C(n) - A(n)) \geqq \lambda(z-\eta)(C(n) - A(n)) \geqq \sum_{m=1}^{z-\eta} D(m) > \frac{\alpha}{2}(2n-z)z - \frac{1}{2}A^2(n).$$

In dieser Zeile ist die erste Ungleichung trivial, die zweite kommt auch in dem obigen Beweis vor, der Beweis der dritten Ungleichung ist für die bei Brauer in Betracht kommenden Werte von n und z mühevoll und wird bei der obigen Beweisanordnung überflüssig.

---

[2]) *Zusatz bei der Korrektur.* Man kann dies folgendermaßen einsehen: Das Schaubild der Funktion $h(\xi)$ besteht aus Teilen einer Geraden und einer Parabel, die an den Stellen $\xi = \pm\eta$ mit $\eta = \sqrt{\alpha\sqrt{\alpha}(2-\sqrt{\alpha})}$ aneinandergefügt sind. Für $\xi > \alpha$ gilt wegen des nach oben konvexen Verlaufs der Parabel und des monotonen Anstiegs der Geraden entweder $h(\xi) > h(\alpha)$ oder $h(\xi) \geqq h(\eta)$. Wegen $0 < \alpha < 1$ und $\lambda \geqq 1$ gilt aber

$$\begin{aligned} h^2(\eta) = \eta^2 &= \alpha\sqrt{\alpha}(2-\sqrt{\alpha}) > \alpha\sqrt{\alpha}(2-\sqrt{\alpha})\left(1-(1-\sqrt{\alpha})^2\right) \\ &= \alpha^2(2-\sqrt{\alpha})^2 \geqq \alpha^2\left(1+\frac{1-\sqrt{\alpha}}{\lambda}\right)^2 = h^2(\alpha). \end{aligned}$$

Also ist für $\xi > \alpha$ stets $h(\xi) > h(\alpha)$.

Eingegangen 16. November 1954.

Unmöglichkeitskernzahlen der kubischen Fermatgleichung mit Primfaktoren der Art $3n+1$ *).

Von *Alexander Aigner* in Graz.

1. Rekapitulation und Vorüberlegung.

In einer vorangehenden Arbeit[1]) habe ich „Unmöglichkeitskernzahlen" angegeben, kurz U-Kernzahlen genannt. Das waren quadratfreie, nur aus Primfaktoren der Art $3n+2$ oder $3n+1$ mit 2 als kubischem Rest bestehende Zahlen $m > 0$ mit der Eigenschaft, daß $x^3 + y^3 = z^3$ in $K(\sqrt{\pm m})$, $K(\sqrt{\pm 3m})$ unmöglich ist, und diese Unmöglichkeit bei Multiplikation mit beliebigen und beliebig vielen Primfaktoren der Art $3n+1$ mit 2 als kubischem Nichtrest stets erhalten bleibt (auch bei durch 3 teilbarer Klassenzahl). Dabei ist immer $m \equiv 1\,(3)$ und es treten beim Aufbau der Zahl m aus ihren Faktoren Gesichtspunkte zutage, welche sich zeichnerisch durch Graphen veranschaulichen lassen. Und zwar kam es auf die Nichtexistenz von Lösungen an; das sind Punktmengen im Graphen, zu denen von jedem Punkt aus eine gerade Anzahl von Linien führt.

Während eine Primzahl der Form $3n+2$ in der Zeichnung einen Punkt darstellt, verfügt eine Primzahl der Form $3n+1$ mit 2 als kubischem Rest an sich über drei Punkte, von denen nach Wahl zwei in die Zeichnung aufzunehmen sind, wobei überdies noch ihre Verbindungslinie willkürlich ist, so daß durch diese Primzahlen größere Mannigfaltigkeit und schwerere Übersicht zustandekommt. Und ich habe für diesen Fall auch nur am Rande ein einfaches Beispiel gebracht ($m = 2 \cdot 31 \cdot 41$). Nun will ich tiefer in die Struktur solcher U-Kernzahlen eindringen.

Bezeichnungsweise. Im folgenden bedeute der Buchstabe p ($p_1, p_2, \ldots$) stets eine Primzahl der Form $3n+1$, für die 2 kubischer Rest ist, und q ($q_1, q_2, \ldots$) eine Primzahl der Form $3n+2$.

Um nun einen geeigneten Überblick über die Graphen mit p-Punkten zu bekommen, stellen wir zunächst zwei Tatsachen fest:

1. Die Summe zweier Punkte derselben Primzahl p entspricht dem dritten (nicht eingezeichneten) Punkt. Im Schema des Graphen kann daher auch mit Lösungen, die beide gezeichneten p-Punkte enthalten, als völlig gleichberechtigt gerechnet werden.

2. Zu einer Lösung des verringerten Systems mit nur einem p-Punkt, die diesen enthält, ist die Stellung des anderen p-Punktes an sich völlig gleichgültig; sie kann durch Verbinden oder Nichtverbinden der beiden p-Punkte gerade eingerichtet werden, so daß also die betreffende Lösung *formal* auch eine Lösung des Gesamtsystems mit beiden p-Punkten ist.

---

*) Vorgetragen auf der Spezialtagung für Zahlentheorie, Mathematisches Forschungsinstitut Oberwolfach, 3.–8. Januar 1955.

[1]) *A. Aigner*, Die kubische Fermatgleichung in quadratischen Körpern, Journ. f. r. u. a. Math. **195** (1955), 3–17.

Und eine U-Kernzahl liegt dann vor, wenn in allen diesen Fällen der Graph keine Lösung hat. Das ist nur bei gerader Punktezahl, also bei gerader q-Punktezahl möglich; deshalb ist auch $m \equiv 1\,(3)$.

Nebenbemerkung. Würde man etwa alle drei p-Punkte einzeichnen, so gäbe es, weil nun eine ungerade Punktezahl vorliegt, immer eine (und nur eine) Lösung. Diese enthält dann aber stets alle drei p-Punkte und eine solche ist in der Tat unbrauchbar. Denn sie führt zwar (durch Weglassung der p-Punkte) zu einer eventuell nicht leeren Menge, welche alle anderen Punkte befriedigt, aber eben — laut Voraussetzung — die p nicht. (Zur Summe der drei p-Punkte liegen alle andern gerade; ob nun diese oder eine andere Menge mit allen p-Punkten schließlich als Lösung erscheint, hängt von der freiwilligen Verbindung der p-Punkte ab.) — Analoges gilt auch beim Einzeichnen von je drei Punkten mehrerer Primzahlen. — Wir erfassen also alle Lösungen bei Einzeichnung von nur zwei Punkten derselben Primzahl.

2. Noch einiges über Graphen.

Nun bringe ich in bezug auf meine Arbeit über Lagebeziehungen in Graphen[2]) und Anwendung dortiger Sätze noch einige auf den hiesigen Zweck gerichtete Resultate.

Die Graphen haben hinsichtlich der Anzahl *aller* Lösungen die Typen 0, 1, 3, 7, 15, . . ., das sind bezüglich der *unabhängigen* Lösungen die Typen 0, 1, 2, 3, 4, . . .; wir wollen in Hinkunft von letzterer Bezeichnungsweise Gebrauch machen. Es ist die Anzahl der unabhängigen Lösungen immer der Anzahl der Punkte mod 2 kongruent. — Bei Umänderung einer Linie (wie auch mehrerer von einem Punkte ausgehender Linien) entsteht nun stets derselbe oder ein übernächster Typ. Und diese Änderung interessiert wegen der freiwilligen Verbindung zweier Punkte derselben Primzahl hier besonders.

Eine genauere Analyse dieser Umänderung, die als Kombination einer Weglassung und einer Anfügung eines Punktes aufgefaßt werden kann, bringt nun das folgende Bild. Zunächst gelten die Regeln:

Zufügen eines Punktes zu allen Lösungen gerade („total positiv") erhöht den Typ um 1.

Zufügen eines Punktes nicht zu allen Lösungen gerade erniedrigt den Typ um 1.

Weglassen eines Punktes, der keiner Lösung angehört, erhöht den Typ um 1.

Weglassen eines Punktes, der einer Lösung angehört, erniedrigt den Typ um 1.

Daraus ergeben sich dafür, daß der Typ bei Änderung einer Linie gleich bleibt, folgende Fälle:

1) Keiner der beiden betroffenen Punkte gehört einer Lösung an und auch keiner einer Lösung des um den anderen Punkt gekürzten Systems. — In diesem Falle hat das System ohne die beiden Punkte den um 2 höheren Typ und aus ihm kann man sich das Gesamtsystem entstanden denken durch zwei nicht total positive, ferner *nicht konforme* Zufügungen, d. h. solche, die nicht zu denselben Lösungen des Grundsystems gerade liegen.
2) Nur einer der beiden Punkte gehört einer Lösung an. — Hier hat das Grundsystem ohne diese Punkte denselben Typ, und das volle entsteht aus ihm entweder durch eine total positive und eine nicht total positive oder durch zwei nicht total positive, aber *konforme* Zufügungen.
3) Beide Punkte gehören einer oder mehr Lösungen an, und zwar jeder solchen beide Punkte zugleich. — Da gilt dasselbe wie in Fall 2).

---

[2]) *A. Aigner*, Einige Sätze über Lagebeziehungen in endlichen Graphen, Journ. f. r. u. a. Math. **195** (1955), 18—21.

Faßt man die Zufügungen nicht simultan, sondern schrittweise auf, also die zweite auf das Zwischensystem bezogen, so kann man auch sagen: Fall 1) besteht aus zwei nicht total positiven, Fall 2) aus einer total positiven und einer nicht total positiven Zufügung in dieser Reihenfolge, Fall 3) in umgekehrter Reihenfolge.

In den anderen denkbaren Fällen bewirkt die Änderung der Linie auch eine Änderung des Typus.

Sodann einiges über das Verhalten der Lösungen bei Summation von Graphen bzw. bei Zerlegung in zusammenhängende Einzelteile. Sogleich ersieht man: Die unabhängigen Lösungen eines nicht zusammenhängenden Graphen sind die seiner zusammenhängenden Bestandteile. Speziell hat also die Summe von lauter Graphen vom Typ 0 wieder diesen Typ. Werden ferner zwei solche getrennte Graphen irgendwie durch eine einzige Linie (Brücke) verbunden, so hat der so entstandene Graph wieder keine Lösung.

Beweis. Seien G_1 und G_2 zwei getrennte Graphen, die Punkte P_1 und P_2 die Brückenköpfe und ferner $S_1 + S_2$ eine Lösung des zusammengesetzten Systems, wobei S_1 Teil von G_1 und S_2 Teil von G_2 ist. Alle andren Punkte außer P_1 und P_2 liegen sicher zu S_1 und S_2 gerade. Nun gibt es zwei Fälle. 1. Fall: S_1 enthält P_1 nicht. Dann liegt P_2 zu S_1 gerade, daher, weil zu $S_1 + S_2$, auch zu S_2. Also wäre S_2 eine Lösung von G_2, gegen die Voraussetzung. — 2. Fall: S_1 enthält P_1. Da S_1 den Punkt P_1 nicht als einzigen Knotenpunkt ungeraden Grades enthalten kann, so liegt auch P_1 zu S_1 gerade, d. h. S_1 wäre eine Lösung von G_1, gegen die Voraussetzung.

Danach fügen sich auch mehrere lösungslose Graphen nach dem Schema einer offenen Kette wieder zu einem solchen zusammen. Noch allgemeiner ist jeder *Baum* (kreisloser Graph) von lösungslosen Graphen wieder vom Typ 0.

Obiges Schema bleibt auch bei Ersatz eines der beiden Punkte P_1 oder P_2 durch den dritten, ihrer Summe entsprechenden Punkt P_3 stets ohne Lösung. Denn durch Weglassen etwa von P_1 entsteht im ganzen eine — innerhalb von G_1 liegende — Lösung. Diese verschwindet aber wieder bei Anfügen des bezüglich G_1 und P_1 äquivalenten Punktes P_3, unabhängig davon, ob man P_2 noch mit P_2 verbindet oder nicht.

3. Die Struktur der Unmöglichkeits-Kernzahlen.

Damit lassen sich schon mannigfache lösungslose Systeme mit p-Punkten, also U-Kernzahlen mit Primfaktoren der Art $3n + 1$, 2 kubischer Rest, konstruieren. Dazu braucht man nur jeden p-Punkt in einen getrennten Graphen vom Typ 0 einzuordnen, welches Schema somit auch ohne Lösung bleibt, wenn man als Brücken die p-Punkte derselben Primzahl miteinander verbindet. Das einfachste derartige Schema wäre etwa eine oder mehrere solcher Ketten

$$\begin{array}{ccccccccc} q_1 & \text{——} & p_1 & p_1 & \text{——} & p_2 & p_2 & \text{——} & p_3 \quad \cdots\cdots \quad p_r \text{——} q_2 \\ \cdots\cdots & & & & & & & & \end{array}$$

an deren Enden q-Primzahlen stehen. Daraus sieht man auch sogleich, daß es *U-Kernzahlen mit einer beliebigen Anzahl von p-Faktoren und beliebig gerader positiver Anzahl von q-Faktoren* gibt. (Ein allfälliger q-Überschuß kann in einen lösungslosen Graphen zusammengefaßt werden.) Hingegen gibt es kein solches Schema mit p-Punkten allein (siehe unten).

Überhaupt hängt viel vom Teilsystem der q-Faktoren und seinem Lösungstyp ab. Dies System heiße etwa Q_{2k}, wo der Index den Typ andeute. Sogleich findet man: Ist $k > A_p$, die Anzahl der p-Faktoren, so sind stets Lösungen vorhanden, also liegt keine U-Kernzahl vor. Denn jeder zugefügte p-Punkt kann den Typ höchstens um 1 herabsetzen.

Interessanterweise gibt es aber auch bei $k = 0$ (und $A_p > 0$) immer Lösungen. Denn füge ich zunächst einen p-Punkt zu Q_0, so entsteht genau eine Lösung, die den p-Punkt enthält. Nun kann ich aber den zweiten p-Punkt durch Verbinden oder Nichtverbinden der beiden p-Punkte zur eben entstandenen Lösung ungerade einfügen, so daß sie wieder verschwindet und der Typ 0 entsteht. So mit weiteren p fortfahrend, läßt sich der lösungslose Zustand bis zum vorletzten Schritt erhalten, worauf dann beim letzten eine brauchbare Lösung entsteht.

Ein Spezialfall davon, in dem sich ebenso verfahren läßt, ist, daß gar keine q vorhanden sind und nur p allein. Damit gilt der Satz:

Ein Produkt aus lauter Primzahlen der Art $3n + 1$ *mit* 2 *als kubischem Rest ist keine U-Kernzahl; für diese Werte bleibt eine entsprechende kubische Fermatgleichung im Prinzip möglich.*

So ist denn auch $x^3 + y^3 = z^3$ in $K(\sqrt{1333})$ lösbar; $1333 = 31 \cdot 43$. — Natürlich fallen auch die genannte Primzahlen selbst darunter.

Das eben geschilderte Verfahren läßt sich auch auf *jede* U-Kernzahl (nicht nur aus q-Faktoren bestehend) als Ausgangspunkt anwenden. Somit ergibt sich der eigenartige Satz:

Eine U-Kernzahl liefert mit einer oder mehreren Primzahlen der Art $3n + 1$, 2 *kubischer Rest, multipliziert nie wieder eine U-Kernzahl.*

So ist z. B. das 10-fache einer solchen Primzahl nie U-Kernzahl und in der Tat wird die Gleichung lösbar für $m = 310, -430, 2230, 2770, 7 \cdot 2830$.

Aus dem Satz geht rein logisch hervor, daß auch eine U-Kernzahl durch eine Primzahl dieser Art *geteilt* nie wieder eine U-Kernzahl ergibt.

Somit erkennen wir die Tatsache, daß nur aus einer Zahl, deren Graph stets *genau zwei* unabhängige Lösungen hat, durch Multiplikation mit einer p-Primzahl eine U-Kernzahl hervorgehen kann. Und zwar so, daß die beiden p-Punkte nicht total positiv und nicht konform (nach Fall 1) in Kapitel 2) angefügt werden. Das bedeutet auch: Von den insgesamt drei p-Punkten liegt jeder zu einer der insgesamt drei Lösungen gerade, und zwar jeder zu einer andern, nach Art einer Paarung.

Und wie muß nun diese Zahl mit dem Graphentyp 2, falls sie selbst noch einen p-Faktor besitzt, weiterhin beschaffen sein? Aus welchen Typen müßte sie ihrerseits durch Multiplikation mit p entstehen? Ihr Graph muß jedenfalls so aussehen, daß er auch bei Änderung der Linie zwischen den p-Punkten invariant vom Typ 2 ist. Und dafür gibt es nach Kapitel 2 nur zwei Möglichkeiten.

1) Entweder ist die Zahl aus einer vom Typ 4 hervorgegangen, und zwar durch zwei nicht total positive, nicht konforme Anfügungen, nach dem dortigen Fall 1). — Wir wollen diese Art der Zufügung kurz als den Operator S bezeichnen.

2) Oder ist sie aus einer Zahl vom selben Typ 2 hervorgegangen, und zwar durch eine total positive und eine andere Anfügung oder durch zwei konforme andere, nach dem dortigen Fall 2), 3). Diese beiden Zufügungsarten sind ohnehin äquivalent; denn hier liegen von den insgesamt drei p-Punkten einer total positiv und zwei anders aber konform zu den drei Lösungen. — Diese Anfügung sei der Operator T genannt.

Und wenn wir den Vorgang noch weiter zurück verfolgen, so kommen wir immer auf diese beiden Operatoren. (Also z. B. Typ 4 durch S aus Typ 6.) — Der dritte an sich mögliche Operator, die total positive Anfügung beider p-Punkte, kann umgangen werden. Denn zunächst ist (nach obigem Satz) weder das Ausgangssystem, noch ein Zwischenresultat vom Typ 0. Zu den also noch vorhandenen Lösungen können aber nicht alle ausständigen p total positiv stehen, weil ja sonst diese Lösungen endgültig verblieben. Mindestens ein p-Faktor muß also mit S oder T anschließen.

Somit läßt sich mit Hilfe der Operatoren S und T, ausgehend von einem System Q_{2k} jede U-Kernzahl darstellen. Q_0 bleibt stets allein; sonst folgt eine beliebige Reihe von S und T (oder nur S), welche k-mal S enthält (weil S den Typ um 2 herabsetzt und T ihn beläßt) und stets mit S schließt, z. B. Q_4TTSTS. Und wie man am besten aus Kettenformen sieht, liefert auch jede solche Darstellung U-Kernzahlen, wenn auch nicht immer *nur* solche. (Dies gilt bei Formen ohne T.) Mitunter hat, obgleich an sich $ST \neq TS$ ist, ein Schema mehrere Darstellungen, natürlich dann mit gleicher Anzahl von S und T. So kann z. B. das Zweikettenschema

$$q_1 \text{——} p_1 \quad p_1 \text{——} p_2 \quad p_2 \text{——} q_2 \qquad q_3 \text{——} p_3 \quad p_3 \text{——} q_4$$

in der Form Q_4STS oder Q_4TSS erhalten werden. (Je nachdem man zuerst p_3 anfügt oder nicht.)

Abschließend sei noch bemerkt, daß jeder Graph auch an Primzahlkombinationen verwirklicht wird, sogar an unendlich vielen. So ist z. B. $11 \cdot 41 \cdot 31 \cdot 43$ eine Unmöglichkeitskernzahl nach dem Schema Q_2TS und $2 \cdot 41 \cdot 53 \cdot 83 \cdot 31 \cdot 43$ eine solche nach Q_4SS. Ihre Strukturformeln haben, durch geeignete Auswahl der p-Punkte auf die Mindestzahl von Linien gebracht, das Aussehen:

$$11 \text{——} 31 \text{——} 41 \text{——} 43 \qquad 43 \text{——} 31 \qquad \text{(Kette)}$$

bzw.

$$\begin{array}{ccccc} 2 & & 31 & & \\ | & & | & \diagdown & \\ 43 & — & 41 & — & 43 \\ | & & | & & \\ 53 & — & 31 & — & 83 \end{array}$$

Eingegangen 29. November 1954.

Über zahlentheoretische Funktionen*).

Von *Hans-Joachim Kanold* in Gießen.

Wir betrachten in dieser Arbeit zahlentheoretische Funktionen, bei denen der Wertevorrat, evtl. bis auf eine endliche Menge von Ausnahmen, eine Untermenge der Menge $\mathfrak{N}$ aller natürlichen Zahlen ist. Mit anderen Worten: Ist n eine beliebige, hinreichend große natürliche Zahl, $f(n)$ eine zahlentheoretische Funktion, so soll auch $f(n)$ eine natürliche Zahl sein. Den Wertevorrat, d. h. genauer, die Menge aller $f(n)$, die natürliche Zahlen sind, wollen wir mit $\mathfrak{F}$ bezeichnen. Bezeichnen wir ferner die Anzahl der (verschiedenen) $f(n) \in \mathfrak{F}$, $f(n) \leqq N$ mit $F(N)$, so definieren wir wie üblich

$$(1) \qquad \overline{\lim_{N\to\infty}} \frac{F(N)}{N} = \overline{D}^*(\mathfrak{F}) \quad \text{bzw.} \quad \underline{\lim_{N\to\infty}} \frac{F(N)}{N} = \underline{D}^*(\mathfrak{F})$$

und nennen diese Grenzwerte die obere bzw. untere asymptotische Dichte der Menge $\mathfrak{F}$. Sind diese beiden Grenzwerte gleich, existiert also

$$(2) \qquad \lim_{N\to\infty} \frac{F(N)}{N} = D^*(\mathfrak{F}),$$

so nennen wir diesen Grenzwert die natürliche Dichte von $\mathfrak{F}$.

Außer den Mengen $\mathfrak{F}$ betrachten wir noch weitere Untermengen von $\mathfrak{N}$, die wir so erklären: Es sei immer mit s eine beliebig wählbare, aber dann festgehaltene natürliche Zahl bezeichnet, die insbesondere von der Veränderlichen n nicht abhängt. Wir betrachten die Mengen $\mathfrak{N}_s \leqq \mathfrak{N}$, die genau aus allen den n bestehen, für die die folgende Bedingung gilt:

(3) *Zu jedem $n \in \mathfrak{N}_s$ gibt es mindestens s paarweise und von n verschiedene Zahlen $n_1, \ldots, n_s$, so daß die Gleichungen $f(n) = f(n_\sigma)$ für $\sigma = 1, \ldots, s$ erfüllt sind.*

Die Anzahl der $n \in \mathfrak{N}_s$, $n \leqq N$ bezeichnen wir mit $N_s(N)$ und erklären entsprechend zu (1) und (2)

$$(4) \qquad \overline{\lim_{N\to\infty}} \frac{N_s(N)}{N} = \overline{D}^*(\mathfrak{N}_s).$$

Diese abgekürzte Schreibweise soll bedeuten: Es stehen links und rechts die oberen Querstriche bzw. die unteren bzw. gar keine.

Im folgenden werden wir die Mengen $\mathfrak{F}$ und $\mathfrak{N}_s$ näher untersuchen. Wir denken uns dabei die Primfaktorenzerlegung einer natürlichen Zahl n immer in der Gestalt

$$(5) \qquad n = \prod_{\varkappa=1}^{k} p_\varkappa^{e_\varkappa} \quad \text{mit} \quad p_1 < p_2 < \cdots < p_k$$

geschrieben. Die Anzahl k der verschiedenen Primteiler von n bezeichnen wir auch mit $V(n)$, den größten quadratischen Teiler von n mit $Q^2(n)$.

---

*) Vorgetragen auf der Spezialtagung für Zahlentheorie im Mathematischen Forschungsinstitut Oberwolfach, 3.–8. Januar 1955.

§ 1. Allgemeinere Sätze über die Mengen $\mathfrak{F}$.

Wir beweisen zuerst den einfachen

Satz 1. *Aus* $\lim\limits_{n\to\infty} \frac{f(n)}{n} = \infty$ *folgt* $D^*(\mathfrak{F}) = 0$.

Beweis. Die Voraussetzung besagt, daß zu jeder positiven, reellen Zahl γ eine natürliche Zahl $N = N(\gamma)$ existiert, so daß

$$f(n) > \gamma n \quad \text{für} \quad n \geqq N \tag{6}$$

gilt. Daraus folgt

$$F(\gamma n) < n \quad \text{für} \quad n \geqq N, \tag{7}$$

d. h. für alle natürlichen Zahlen $m \geqq \gamma N$ ist $F(m) \leqq \frac{m}{\gamma}$, also

$$\overline{\lim_{m\to\infty}} \frac{F(m)}{m} = \bar{D}^*(\mathfrak{F}) \leqq \frac{1}{\gamma}. \tag{8}$$

Da wir aber γ beliebig groß wählen können, ergibt sich aus (8) sogleich die Behauptung von Satz 1.

Wir fordern im nächsten Satz von $f(n)$ die Distributivität.

Satz 2. *Die Funktion $f(n)$ erfülle die Bedingungen:*

a) *Aus* $(n_1, n_2) = 1$ *folgt* $f(n_1 n_2) = f(n_1) f(n_2)$.

b) *Es existiere eine feste natürliche Zahl $a > 1$ so, daß $a \mid f(p)$ für alle Primzahlen p gilt, die eine gegebene Konstante K übertreffen.*

c) *Es sei* $\underline{\lim}\limits_{n\to\infty} \frac{f(n)}{n} > 0$.

Dann ist $D^*(\mathfrak{F}) = 0$.

Beweis. Es sei $\underline{\lim}\limits_{n\to\infty} \frac{f(n)}{n} = l > 0$. Dann ist

$$\frac{f(n)}{n} > \frac{l}{2}, \quad \text{d. h.} \quad f(n) > \frac{l}{2} n \quad \text{für alle} \quad n \geqq N_0. \tag{9}$$

Wir spalten nun die Menge $\mathfrak{N}$ aller natürlichen Zahlen n in zwei elementefremde Untermengen $\mathfrak{N}^{(1)}$, $\mathfrak{N}^{(2)}$ auf, die wir so erklären: $\mathfrak{N}^{(1)}$ enthalte genau alle n, bei denen in der Zerlegung (5) mindestens S Primzahlen, die K übertreffen, in der ersten Potenz auftreten. Dabei ist S eine beliebig wählbare, dann festgehaltene natürliche Zahl. $\mathfrak{N}^{(2)}$ ist die Komplementärmenge von $\mathfrak{N}^{(1)}$. Wir ordnen jedem $n \in \mathfrak{N}^{(i)}$ den Wert $f(n)$ zu und bezeichnen die Menge aller dieser $f(n)$ mit $\mathfrak{F}_i$ $(i = 1, 2)$. Aus (9) ergibt sich

$$\bar{D}^*(\mathfrak{F}_i) \leqq \frac{2}{l} \bar{D}^*(\mathfrak{N}^{(i)}) \qquad (i = 1, 2). \tag{10}$$

Ferner ist

$$\bar{D}^*(\mathfrak{F}) \leqq \bar{D}^*(\mathfrak{F}_1) + \bar{D}^*(\mathfrak{F}_2). \tag{11}$$

Da $\mathfrak{F}_1$ nur Zahlen enthält, die wegen der Bedingung b) unseres Satzes durch a^S teilbar sind, folgt sofort

$$\bar{D}^*(\mathfrak{F}_1) \leqq \frac{1}{a^S} \leqq \frac{1}{2^S}. \tag{12}$$

Nach einem bereits an anderer Stelle bewiesenen Satz[1]) ist $\bar{D}^*(\mathfrak{N}^{(2)}) = 0$. Aus (10) und (11) erhalten wir also

$$\bar{D}^*(\mathfrak{F}) \leqq \frac{1}{2^S}. \tag{13}$$

---

[1]) *H. J. Kanold*, Über die Dichten der Mengen der vollkommenen und der befreundeten Zahlen. Math. Z. 61, 180–185 (1954), insbesondere Satz 2.

Weil wir durch passende Wahl von S die rechte Seite von (13) beliebig klein machen können, folgt somit die Behauptung von Satz 2. Durch eine leichte Abänderung der Voraussetzungen erhalten wir

Satz 3. *Die Funktion $f(n)$ erfülle die Bedingungen:*

a) *Aus $(n_1, n_2) = 1$ folgt $f(n_1 n_2) = f(n_1) f(n_2)$.*

b) *Es existiere eine feste natürliche Zahl $a > 1$ so, daß $a \mid f(p^\alpha)$ gilt für jede natürliche Zahl α und jede Primzahl $p > K$.*

c) Es sei $\varliminf\limits_{n\to\infty} \dfrac{f(n)}{\dfrac{n}{\log\log n}} > 0$.

Dann ist $D^*(\mathfrak{F}) = 0$.

Beweis. Wir spalten wieder $\mathfrak{N}$ in zwei Untermengen $\mathfrak{N}^{(1)}$ und $\mathfrak{N}^{(2)}$ auf. $\mathfrak{N}^{(1)}$ enthalte alle n, bei denen in (5)

$$k = V(n) \geqq \pi(K) + S \tag{14}$$

gilt. Dabei bedeutet $\pi(K)$, wie üblich, die Anzahl der Primzahlen, die K nicht übertreffen. $\mathfrak{N}^{(2)}$ ist wieder die Komplementärmenge von $\mathfrak{N}^{(1)}$. Es gelten auch hier die Abschätzungen (11) und (12). Nach bekannten Ergebnissen[2]) ist die Anzahl $A_2(N)$ der $n \in \mathfrak{N}^{(2)}$, $n \leqq N$ kleiner als $\dfrac{N(\log\log N)^{S'}}{\log N}$, wobei zur Abkürzung $\pi(K) + S - 1 = S'$ geschrieben ist. Aus der Bedingung c) folgt

$$\varliminf_{n\to\infty} \frac{f(n)}{\dfrac{n}{\log\log n}} = l > 0; \quad f(n) > \frac{l}{2}\frac{n}{\log\log n} \text{ für } n \geqq N_0. \tag{15}$$

Ist jetzt $N \geqq N_0$, so ist die Anzahl der $f(n) \leqq \dfrac{l}{2}\dfrac{N}{\log\log N}$, $n \in \mathfrak{N}^{(2)}$ kleiner als $\dfrac{N(\log\log N)^{S'}}{\log N}$. Setzen wir

$$\left[\frac{l}{2}\frac{N}{\log\log N}\right] = m, \tag{16}$$

so ist die Anzahl $F_2(m)$ der $f(n) \leqq m$, $n \in \mathfrak{N}^{(2)}$ kleiner als $m \cdot \dfrac{2}{l} \cdot \dfrac{(\log\log N)^{S'+1}}{\log N} = o(m)$. Das bedeutet aber

$$\overline{D}^*(\mathfrak{F}_2) = 0. \tag{17}$$

Daraus folgt (13) und somit der vollständige Beweis von Satz 3.

§ 2. Allgemeinere Sätze über die Mengen $\mathfrak{N}_s$.

Wir beginnen mit dem einfachen

Satz 4. *Aus $\lim\limits_{n\to\infty} \dfrac{f(n)}{n} = 0$ folgt $D^*(\mathfrak{N}_s) = 1$.*

Beweis. Die Voraussetzung besagt, daß zu jedem $\varepsilon > 0$ eine natürliche Zahl $N_0 = N_0(\varepsilon)$ existiert, so daß

$$f(n) < \varepsilon n \text{ für } n \geqq N_0 \tag{18}$$

gilt. Daraus folgt für die Komplementärmenge $\mathfrak{K}_s$ von $\mathfrak{N}_s$

$$\overline{D}^*(\mathfrak{K}_s) \leqq \varepsilon s. \tag{19}$$

[2]) *E. Landau*, Handbuch der Lehre von der Verteilung der Primzahlen, Leipzig u. Berlin 1909, S. 209ff.

Weil wir ε beliebig klein wählen können, folgt

$$\overline{D}^*(\mathfrak{K}_s) = D^*(\mathfrak{K}_s) = 0. \tag{20}$$

Damit ist aber

$$D^*(\mathfrak{N}_s) = 1 \tag{21}$$

als richtig erkannt.

Satz 5. *Genügt $f(n)$ den Bedingungen $D^*(\mathfrak{F}) = 0$ und $\sum\limits_{n \leq N} \frac{f(n)}{n} = O(N)$,* so ist $D^*(\mathfrak{N}_s) = 1$.

Beweis. Es sei $\mathfrak{K}_s$ die Komplementärmenge von $\mathfrak{N}_s$. Wir müssen zeigen, daß $D^*(\mathfrak{K}_s) = 0$ gilt. Zu jedem $n \in \mathfrak{K}_s$ existieren höchstens $s - 1$ Zahlen $n_1, \ldots, n_{s-1}$ derart, daß

$$f(n) = f(n_1) \equiv \cdots = f(n_{s-1}) \tag{22}$$

erfüllt ist. Wir spalten $\mathfrak{K}_s$ in zwei elementefremde Teilmengen $\mathfrak{K}_s^{(1)}$, $\mathfrak{K}_s^{(2)}$ auf. Es sei

$$f(n) \leqq Kn \text{ für alle } n \in \mathfrak{K}_s^{(1)}, \tag{23}$$

wobei K eine vorgegebene natürliche Zahl sein soll. Es sei

$$f(n) > Kn \text{ für alle } n \in \mathfrak{K}_s^{(2)}. \tag{24}$$

Die Anzahl der $n \in \mathfrak{K}_s^{(1)}$, $n \leqq N$ ist höchstens gleich dem s-fachen der Anzahl der $f(n) \leqq KN$, $n \in \mathfrak{K}_s^{(1)}$. Wir haben somit

$$\overline{D}^*(\mathfrak{K}_s^{(1)}) \leqq Ks\overline{D}^*(\mathfrak{F}_1), \tag{25}$$

wenn wir mit $\mathfrak{F}_1$ die Menge der $f(n)$, $n \in \mathfrak{K}_s^{(1)}$ bezeichnen.

Wegen $\overline{D}^*(\mathfrak{F}_1) \leqq \overline{D}^*(\mathfrak{F}) = D^*(\mathfrak{F}) = 0$ folgt daraus

$$D^*(\mathfrak{K}_s^{(1)}) = 0. \tag{26}$$

Bezeichnen wir nun mit $A_K(N)$ die Anzahl der $n \in \mathfrak{K}_s^{(2)}$, $n \leqq N$, so erhalten wir nach (24)

$$KA_K(N) < \sum_{n \leq N} \frac{f(n)}{n} < CN, \tag{27}$$

wobei C eine feste Konstante bedeutet. Daraus ergibt sich

$$\frac{A_K(N)}{N} < \frac{C}{K}. \tag{28}$$

Wählen wir speziell $K > \frac{1}{\varepsilon} C$, $\varepsilon > 0$, so ist

$$\overline{D}^*(\mathfrak{K}_s^{(2)}) \leqq \varepsilon, \tag{29}$$

also, weil $\varepsilon > 0$ beliebig klein sein kann, auch

$$D^*(\mathfrak{K}_s^{(2)}) = 0. \tag{30}$$

Aus (26) und (30) folgt $D^*(\mathfrak{K}_s) = 0$ und somit der vollständige Beweis von Satz 5.

§ 3. Anwendungen auf spezielle Funktionen.

Wir wollen die Sätze der vorangehenden Paragraphen auf einige der wichtigsten zahlentheoretischen Funktionen anwenden und betrachten zunächst die Teilerfunktionen

$$\sigma_r(n) = \sum_{d \mid n} d^r \qquad (r = 0, 1, 2, \ldots). \tag{31}$$

Diese sind distributiv. Bekanntlich liefert $r = 0$ die *Anzahl* der Teiler

$$\sigma_0(n) = \tau(n) = \sum_{d|n} 1 \tag{32}$$

und $r = 1$ die *Summe* der Teiler

$$\sigma_1(n) = \sigma(n) = \sum_{d|n} d. \tag{33}$$

Für $r > 1$ ist $\sigma_r(n) \geqq n^r$, d. h. $\lim\limits_{n\to\infty} \frac{\sigma_r(n)}{n} = \infty$. Nach Satz 1 ist also $D^*(\mathfrak{F}) = 0$.

Für $r = 1$ ist $\frac{\sigma(n)}{n} \geqq 1$, also $\varliminf\limits_{n\to\infty} \frac{\sigma(n)}{n} > 0$. Ferner ist $2 \mid \sigma(p) = 1 + p$ für $p > 2$. Nach Satz 2 ist daher auch hier $D^*(\mathfrak{F}) = 0$. Aus

$$\sum_{n \leq N} \frac{\sigma(n)}{n} = \sum_{n \leq N} \sum_{d|n} \frac{1}{d} = \sum_{n \leq N} \left[\frac{N}{n}\right] \frac{1}{n} < \frac{\pi^2}{6} N = O(N) \tag{34}$$

und Satz 5 folgt auch $D^*(\mathfrak{N}_s) = 1$.

Für $r = 0$ folgt $\tau(p^\alpha) = \alpha + 1$. Hierin kann α jeden der Werte $0, 1, \ldots$ annehmen, $\alpha + 1$ also jede natürliche Zahl sein. Das bedeutet aber $D^*(\mathfrak{F}) = 1$. Nach einem bekannten Satz [3]) ist

$$\varlimsup_{n\to\infty} \frac{\log \tau(n)}{\frac{\log n}{\log\log n}} = \log 2, \tag{35}$$

also $\lim\limits_{n\to\infty} \frac{\tau(n)}{n} = 0$. Damit folgt nach Satz 4 sogleich auch $D^*(\mathfrak{N}_s) = 1$.

Für die Anzahl $\pi(n)$ aller Primzahlen, die n nicht übertreffen, ist sofort klar, daß $D^*(\mathfrak{F}) = 1$ sein muß. Aus dem Primzahlsatz folgt sogleich $\lim\limits_{n\to\infty} \frac{\pi(n)}{n} = 0$ und damit nach Satz 4 ebenfalls $D^*(\mathfrak{N}_s) = 1$.

Zum Schluß betrachten wir die Eulersche φ-Funktion. Diese ist distributiv. Ferner gilt [4])

$$\varliminf_{n\to\infty} \frac{\varphi(n)}{\frac{n}{\log\log n}} = e^{-C} > 0; \tag{36}$$

dabei ist C die Eulersche Konstante. Weiterhin ist

$$2 \mid \varphi(p^\alpha) = (p - 1)\, p^{\alpha-1} \quad \text{für} \quad \alpha > 0,\ p > 2. \tag{37}$$

Nach Satz 3 ist sofort zu sehen, daß $D^*(\mathfrak{F}) = 0$ sein muß. Weil $\frac{\varphi(n)}{n} \leqq 1$, also $\sum\limits_{n \leq N} \frac{\varphi(n)}{n} = O(N)$ gilt, liefert Satz 5 unmittelbar $D^*(\mathfrak{N}_s) = 1$.

§ 4. Verallgemeinerungen bekannter Fragestellungen.

Wir betrachten die folgende Fragestellung, die einige seit langer Zeit in der Zahlentheorie gestellte Probleme umfaßt [5]).

[3]) Vgl. a. a. O. [2]), S. 220.

[4]) Vgl. a. a. O. [2]), S. 216/17.

[5]) *L. E. Dickson*, Amicable number triples. Bull. Amer. Math. Soc. (2), **19** (1912), 285–86.
T. E. Mason, On amicable numbers and their generalizations. Bull. Amer. Math. Soc. (2) **27** (1920), 305.

Es sei $f(n)$ eine zahlentheoretische Funktion. Wir betrachten das System von Gleichungen

$$(*) \qquad f(n_1) = f(n_2) = \cdots = f(n_t);$$

$$(**) \qquad f(n_1) = \sum_{\tau=1}^{t} u_\tau n_\tau.$$

Dabei seien die u_τ ganze oder natürliche oder auch nur rationale Zahlen, die entweder vorgegeben sind oder gewissen einschränkenden Bedingungen unterworfen werden. Gefragt ist nach den Systemen von je t natürlichen Zahlen n_τ, die (*) und (**) befriedigen. Wir sehen sofort: Ist für die Funktion $f(n)$ die Aussage $\overline{D}^*(\mathfrak{N}_{t-1}) > 0$ gültig, so ist (*) für unendlich viele Systeme $n_1, \ldots, n_t$ erfüllt. $D^*(\mathfrak{N}_{t-1}) = 1$ besagt, daß „fast alle" natürlichen Zahlen zu mindestens einem Lösungssystem von (*) gehören. Dabei bedeutet „fast alle", wie üblich, „alle, bis auf eine Menge mit der natürlichen Dichte Null".

Wir betrachten jetzt kurz noch zwei Sonderfälle.

I. $t = 1$. Dann reduzieren sich (*) und (**) auf

$$(38) \qquad f(n) = un.$$

Ist hierin $f(n) = \sigma(n)$ und $u > 1$ eine natürliche Zahl, so sind die Lösungen von (38) die vollkommenen und mehrfach vollkommenen Zahlen. An anderer Stelle [6]) wurde gezeigt, daß die Menge dieser Zahlen die natürliche Dichte Null besitzt. Dieses Ergebnis werden wir in dem folgenden Paragraphen verallgemeinern.

II. $t = 2$. Die Bedingungsgleichungen (*) und (**) nehmen jetzt die folgende Gestalt an:

$$(39) \qquad f(n_1) = f(n_2);$$

$$(40) \qquad f(n_1) = u_1 n_1 + u_2 n_2.$$

Setzen wir hierin wieder $f(n) = \sigma(n)$ und außerdem $u_1 = u_2 = 1$, so sind die Lösungen von (39) und (40) die befreundeten Zahlenpaare. Wie früher bewiesen wurde [7]), besitzt die Menge dieser Zahlen eine obere asymptotische Dichte, die unterhalb von 0,204 liegt. Wir werden den Fall $t = 2$ in § 6 näher untersuchen.

§ 5. Der Fall $t = 1$.

Wir befassen uns jetzt etwas genauer mit der Diskussion von (38). Für u wollen wir rationale Zahlen zulassen. Es sei also $u = \frac{v}{w}$. Wir schreiben dann statt (38)

$$(41) \qquad wf(n) = vn$$

und sehen sofort, daß wir uns auf $w > 0$ und $v > 0$ sowie $(v, w) = 1$ beschränken dürfen. Eine erste Aussage gibt

Satz 6. *Es seien v und w vorgegebene natürliche Zahlen. Die Funktion $f(n)$ erfülle die Bedingungen* a) *und* b) *aus Satz* 2. *Bezeichnen wir mit $\mathfrak{L}$ die Menge aller Lösungen n von* (41), *so ist $D^*(\mathfrak{L}) = 0$.*

Beweis. Nach einem früheren Satz [8]) brauchen wir nur solche n zu betrachten, für die $a^{2h} \mid f(n)$ gilt, wobei h eine beliebig große, vorgegebene Schranke bedeutet. Wählen

[6]) *H. J. Kanold*, Über mehrfach vollkommene Zahlen. Journ. f. reine u. angew. Math. **194** (1955), 218–220, Satz 2.

[7]) A. a. O. [1]), insbesondere Satz 4.

[8]) A. a. O. [1]).

wir h so groß, daß $a^h \geqq v$ ist, so folgt $a^h \mid n$. Die Dichte aller dieser n ist aber nicht größer als $\frac{1}{a^h}$, sie kann also durch passende Wahl von h beliebig klein gemacht werden. Damit ist Satz 6 bewiesen. Betrachten wir nun die Gleichung

$$w(n)\, f(n) = v(n)\, n, \tag{42}$$

d. h. lassen wir $u = \frac{v}{w}$ von n abhängen, so sehen wir aus dem Beweis von Satz 6, daß die Menge aller Lösungen von (42) auch die Dichte Null besitzt, wenn nur $v(n)$ beschränkt bleibt; ja sogar auch dann noch, wenn wenigstens eine feste natürliche Zahl S so existiert, daß $a^S \nmid v(n)$ für alle n gilt.

Eine weitere Verschärfung ergibt

Satz 7. *In* (42) *seien die* $w(n)$ *nach oben beschränkt; ferner sei außer den Voraussetzungen* a) *und* b) *aus Satz* 2 *noch erfüllt:* $\sum_{n \leq N} \frac{f(n)}{n} = O(N)$. *Dann ist* $D^*(\mathfrak{L}) = 0$.

Beweis. Die Voraussetzung $\sum_{n \leq N} \frac{f(n)}{n} = O(N)$ besagt: Es existiert eine Konstante C so, daß für alle N gilt $\sum_{n \leq N} \frac{f(n)}{n} < CN$. Es sei S nun eine vorgegebene Schranke. Aus $\frac{f(n)}{n} = \frac{v(n)}{w(n)} \leqq S$ folgt $v(n) \leqq S w(n)$, d. h. $v(n)$ bleibt beschränkt. Nach den obigen Überlegungen können wir die Menge dieser n vernachlässigen. Wir betrachten also von nun an nur diejenigen n, für die $\frac{f(n)}{n} > S$ ist. Es sei deren Anzahl unterhalb $N + 1$ gleich $A(N)$. Wir erhalten dann

$$S A(N) < \sum_{n \leq N} \frac{f(n)}{n} < CN. \tag{43}$$

Aus (43) ergibt sich

$$\frac{A(N)}{N} < \frac{C}{S}. \tag{44}$$

Durch passende Wahl von S läßt sich die rechte Seite beliebig klein machen. Daraus folgt die Richtigkeit von Satz 7.

Satz 8. $f(n)$ *habe die Eigenschaften* a) *und* b) *aus Satz* 2. *Ferner sei* $f(p_i^\alpha) < f(p_j^\alpha)$ *für je zwei Primzahlen* $p_i < p_j$ *und jede natürliche Zahl* α. *Dann gilt: Fast alle* n — *die wir uns in der Zerlegung* (5) *geschrieben denken — besitzen die Eigenschaft, daß* $f(n)$ *nur Primteiler hat, die* $\frac{1}{a} f(p_k)$ *nicht übertreffen.*

Beweis. Wir zeigen, daß die Komplementärmenge die Dichte Null besitzt. Es sei n ein Element der Komplementärmenge, das wir uns mit der Zerlegung (5) dargestellt denken. Dann existiert eine Primzahl q derart, daß q den folgenden beiden Bedingungen genügt:

$$q > \frac{1}{a} f(p_k); \tag{45}$$

$$q \mid f(p_\varkappa^{\alpha_\varkappa}) \text{ für mindestens ein } \varkappa \text{ aus } 1, \ldots, k. \tag{46}$$

Wir können annehmen[9]), daß p_k größer als eine beliebig vorgegebene Schranke ist. Wegen $f(p_1) < f(p_2) < \cdots < f(p_k)$ können wir weiterhin annehmen, daß auch $\frac{1}{a} f(p_k)$ sehr groß,

[9]) A. a. O. [1]).

und nach (45), daß auch q sehr groß ist. Bezeichnen wir mit $q_1 < q_2 < \cdots$ die Folge aller, der Größe nach geordneten Primzahlen, so soll q die Ungleichungen

$$(47) \qquad q > a; \quad q > f(q_{\pi(S)}^{\alpha}) \quad \text{mit} \quad \alpha \leqq S$$

sämtlich erfüllen. Dabei sei S eine beliebig vorgegebene Schranke und $q_{\pi(S)} \leqq S < q_{\pi(S)+1}$.

Ist in (46) der Exponent $\alpha_\varkappa$ gleich 1, so erhalten wir aus

$$(48) \qquad f(p_k) \geqq f(p_\varkappa) \geqq aq > a\frac{1}{a} f(p_k)$$

sogleich einen Widerspruch.

Ist in (46) der Exponent $\alpha_\varkappa$ größer als 1, so liefert dies nach (47)

$$(49) \qquad f(p_\varkappa^{\alpha_\varkappa}) \geqq q > f(q_{\pi(S)}^{\alpha}).$$

Wir schätzen nun den größten quadratischen Teiler von n ab.

Aus $p_\varkappa > q_{\pi(S)}$ folgt $Q^2(n) \geqq p_\varkappa^2 > S^2$. Aus $p_\varkappa \leqq q_{\pi(S)}$ folgt $Q^2(n) \geqq 2^S$.

Wir brauchen also nur noch zu zeigen, daß eine Menge natürlicher Zahlen, bei der jedes Element einen quadratischen Teiler besitzt, der größer als eine beliebig vorgegebene Schranke d^2 ist, eine obere asymptotische Dichte hat, die kleiner als $\frac{6}{\pi^2 d}$ ist. Das folgt aber aus einem früheren Satz[10]). Danach ist diese Dichte höchstens gleich

$$1 - \frac{6}{\pi^2} \sum_{j=1}^{d} \frac{1}{j^2} < \frac{6}{\pi^2 d}.$$

Hiermit ist der Beweis von Satz 8 beendet.

Wir wollen jetzt noch die Sätze dieses Paragraphen auf die in § 3 angeführten Funktionen anwenden. Wir sehen sofort, daß die Funktionen $\varphi(n)$ und $\sigma_r(n)$ $(r = 0, 1, 2, \ldots)$ die Bedingungen a) und b) aus Satz 2 erfüllen. Also gilt für alle diese Funktionen der Satz 6. Dieser gilt natürlich auch für $\pi(n)$. Denn die Gleichung

$$(50) \qquad w\pi(n) = vn$$

hat nach dem Primzahlsatz bei vorgegebenen v und w nur endlich viele Lösungen. Die zusätzliche Bedingung von Satz 7 erfüllen die Funktionen $\tau(n)$, $\sigma(n)$, $\varphi(n)$. Also gilt für sie der Satz 7. Wiederum folgt aus dem Primzahlsatz, daß dies auch der Fall ist für $\pi(n)$. Die Funktionen $\varphi(n)$ und $\sigma_r(n)$ $(r > 0)$ erfüllen die Bedingungen von Satz 8. Dagegen sieht man leicht ein, daß für $\tau(n)$ der Satz 8 nicht gilt, denn es ist $\frac{1}{a}\tau(p_k) = \frac{1}{2} \cdot 2 = 1$.

§ 6. Der Fall $t = 2$.

Wir untersuchen nun die Gleichungen (39) und (40) etwas eingehender. Da $n_1 = n_2 = n$ auf den Fall $t = 1$ führt, können wir annehmen

$$(51) \qquad n_1 < n_2.$$

Sind u_1, u_2 gegebene rationale Zahlen, so ergeben (39) und (40)

$$(52) \qquad u_2 n_2 = f(n_1) - u_1 n_1; \quad u_1 n_1 = f(n_2) - u_2 n_2.$$

[10]) *H. J. Kanold*, Über die Dichte von gewissen Zahlenmengen. Journ. f. reine u. angew. Math. 193 (1954), 250—252, Hilfssatz 1.

Bei gegebenem n_1 und $u_2 \neq 0$ ist also n_2 eindeutig bestimmt; bei gegebenem n_2 und $u_1 \neq 0$ ist n_1 eindeutig bestimmt. $u_2 = 0$ ergibt die Bedingungen $f(n_1) = f(n_2) = u_1 n_1$; $u_1 = 0$ ergibt $f(n_1) = f(n_2) = u_2 n_2$. Davon besagt $f(n_1) = f(n_2)$, daß die Lösungen Elemente der Menge $\mathfrak{N}_1$ sind. Die Bedingung $f(n_i) = u_i n_i$ für $i = 1$ bzw. $i = 2$ haben wir bereits in § 5 behandelt. Wir setzen daher von jetzt an voraus

$$u_1 u_2 \neq 0. \tag{53}$$

Bezeichnen wir mit $\mathfrak{L}$ die Menge aller Lösungen von (39) und (40), mit $\mathfrak{L}_1$ die Untermenge aller n_1, mit $\mathfrak{L}_2$ die Untermenge aller n_2, so folgt aus (51), (52) und (53)

$$\overline{D}^*(\mathfrak{L}) \leqq \overline{D}^*(\mathfrak{L}_1) + \overline{D}^*(\mathfrak{L}_2) \leqq 2\overline{D}^*(\mathfrak{L}_1). \tag{54}$$

Wenn wir $\overline{D}^*(\mathfrak{L}_1)$ nach oben abschätzen wollen, können wir eine Untermenge von $\mathfrak{L}_1$ der asymptotischen Dichte Null vernachlässigen. Wir brauchen also nur solche n_1 zu betrachten, für die $V(n_1)$ oberhalb einer vorgegebenen Schranke liegt, und die wenigstens $2S$ Primzahlen $> K$ in genau der ersten Potenz enthalten[11]). Genügt $f(n)$ den Bedingungen a) und b) aus Satz 2, so gilt also für die Zahlen n_1

$$a^{2S} \mid f(n_1). \tag{55}$$

Daraus folgt aber sogleich nach (52)

$$u_1 n_1 + u_2 n_2 \equiv 0 \bmod a^{2S}. \tag{56}$$

Sind u_1, u_2 zwei vorgegebene ganze Zahlen, die (53) erfüllen, so können wir S so groß wählen, daß $a^S > u_i$ wird für $i = 1, 2$. Ferner können wir annehmen, daß $u_1 n_1$ und $u_2 n_2$ die Zahl a in der gleichen Potenz enthalten. Denn sei z. B.

$$a^\xi \mid u_1 n_1; \quad a^{\xi+1} \nmid u_1 n_1; \quad a^\eta \mid u_2 n_2; \quad a^{\eta+1} \nmid u_2 n_2; \quad \xi < \eta. \tag{57}$$

Dann folgt aus (56)

$$\eta > 2S; \quad \xi = 2S. \tag{58}$$

Das führt zu $a^S \mid n_i$ für $i = 1, 2$. Die Dichte aller durch a^S teilbaren Zahlen ist aber $\frac{1}{a^S}$, d. h. bei passend gewähltem S beliebig klein. Wir beweisen nun den folgenden

Satz 9. *Die Menge $\mathfrak{N}'$ bestehe aus allen natürlichen Zahlen n, bei denen $k = V(n)$ eine feste Schranke S nicht überschreitet und bei denen außerdem $\max\limits_{\varkappa=1}^{k} \alpha_\varkappa > 1$ ist bei der Zerlegung* (5). *Es sei u eine gegebene natürliche Zahl. Wir ordnen jedem $n \in \mathfrak{N}'$ eine Zahl $m = f(n)$ — un zu. Für die Menge $\mathfrak{M}$ der „zugehörigen" m ist dann $D^*(\mathfrak{M}) = 0$, wenn $f(n)$ die Bedingung $f(n) \geqq n \cdot \frac{up_1 + 1}{p_1}$ für alle $n \in \mathfrak{N}'$ erfüllt.*

Beweis. Wir spalten die Menge $\mathfrak{N}'$ in S Teilmengen auf: $\mathfrak{N}_i'$ enthält genau die $n \in \mathfrak{N}'$ mit $\alpha_1 = \alpha_2 = \cdots = \alpha_{i-1} = 1$; $\alpha_i > 1$ $(i = 1, \ldots, S)$. Die „zugehörigen" Mengen der m bezeichnen wir mit $\mathfrak{M}_i$. Wir greifen jetzt ein bestimmtes $\mathfrak{N}_i'$ heraus. Jedem $n \in \mathfrak{N}_i'$ ordnen wir *eineindeutig* eine Zahl $n' = \frac{n}{p_i}$ zu. Es ist

$$n' = \frac{n}{p_1} \frac{p_1}{p_i} \leqq \frac{p_1}{p_i} m \leqq m. \tag{59}$$

Daraus folgt für die Menge $\mathfrak{N}_i''$ dieser n'

$$\overline{D}^*(\mathfrak{M}_i) \leqq \overline{D}^*(\mathfrak{N}_i''). \tag{60}$$

[11]) A. a. O. [1]).

Nach früheren Ergebnissen[12]) ist $\bar{D}^*(\mathfrak{N}_i'') = 0$. Also ist auch

$$\bar{D}^*(\mathfrak{M}) \leqq \sum_{i=1}^{S} \bar{D}^*(\mathfrak{M}_i) = 0. \tag{61}$$

Eine Ergänzung zu Satz 9 liefert der

Satz 10. *Die Menge $\mathfrak{N}'$ bestehe aus allen natürlichen Zahlen $n = p_1 p_2 \cdots p_k$, $p_1 < \cdots < p_k$, $k = V(n) \leqq S$. Außerdem sollen alle p_1 eine feste Schranke T nicht überschreiten. u, $f(n)$, m, $\mathfrak{M}$ seien definiert und erfüllen die gleichen Bedingungen wie in Satz 9. Dann ist ebenfalls $D^*(\mathfrak{M}) = 0$.*

Beweis. Wir ordnen jedem $n \in \mathfrak{N}'$ die Zahl $n' = \dfrac{n}{p_1}$ zu. Diese Zuordnung ist eindeutig, aber nicht mehr eineindeutig. Die Anzahl der Primzahlen, die T nicht überschreiten, ist $\pi(T) = T'$. Zu jedem $n' = p_2 p_3 \cdots p_k$ können höchstens T' Zahlen n gehören. Aus $n' \leqq m$ ergibt sich somit

$$\bar{D}^*(\mathfrak{M}) \leqq T' \bar{D}^*(\mathfrak{N}''), \tag{62}$$

wobei N'' die Menge aller n' sei. Da, wie beim Beweis von Satz 9, $\bar{D}(\mathfrak{N}'') = 0$ ist, folgt aus (62) sofort die Behauptung von Satz 10.

Wir vervollständigen jetzt die Sätze 9 und 10, indem wir uns von der einschränkenden Voraussetzung $k = V(n) \leqq S$ befreien. Es sei also von nun an für alle n einer Menge $\mathfrak{N}'$

$$k = V(n) > S \text{ (hinreichend groß)} \tag{63}$$

angenommen. Stets erfülle $f(n)$ die Bedingung aus Satz 9. Dann beweisen wir

Satz 11. *Gelten für alle $n \in \mathfrak{N}'$ die Ungleichungen* (63) *und* $\max\limits_{\varkappa=1}^{S} \alpha_\varkappa > 1$; $\max\limits_{\varkappa=S+1}^{k} \alpha_\varkappa > 1$, *so ist* $\bar{D}^*(\mathfrak{M}) < \dfrac{12}{\pi^2 \log S}$.

Beweis. Wir spalten $\mathfrak{N}'$ wie im Beweis von Satz 9 in die gleichen S Teilmengen $\mathfrak{N}_i'$ auf. Es gilt auch hier die Abschätzung (60). Für $\mathfrak{N}_i''$ ist jetzt aber

$$\bar{D}^*(\mathfrak{N}_i'') \leqq 1 - \frac{6}{\pi^2} \sum_{j=1}^{p_{S+1}-1} \frac{1}{j^2} < \frac{6}{\pi^2} \frac{1}{p_{S+1} - 1} \tag{64}$$

erfüllt. Also erhalten wir

$$\bar{D}^*(\mathfrak{M}) \leqq \sum_{i=1}^{S} \bar{D}^*(\mathfrak{N}_i'') < \frac{6}{\pi^2} \sum_{i=1}^{S} \frac{1}{q_{S+1} - 1}, \tag{65}$$

wobei q_{S+1} wieder die $(S+1)$-te Primzahl (der Größe nach geordnet) sein soll. Für genügend große S ist nun nach dem Primzahlsatz bestimmt immer

$$q_{S+1} - 1 > \frac{S}{2} \log S. \tag{66}$$

Das ergibt mit (65) die Behauptung von Satz 11.

Eine Erweiterung von Satz 10 ist

Satz 12. *Gilt für alle $n \in \mathfrak{N}'$ die Bedingung $p_1 \leqq T$, so ist $\bar{D}^*(\mathfrak{M}) \leqq T' T \bar{D}^*(\mathfrak{N}')$.*

Beweis. Wie beim Beweis von Satz 10 gilt auch jetzt die Abschätzung (62). Wegen der Voraussetzung $p_1 \leqq T$ ist ferner

$$\bar{D}^*(\mathfrak{N}'') \leqq T \bar{D}^*(\mathfrak{N}'). \tag{67}$$

[12]) A. a. O. [1]).

Somit erhalten wir

$$\bar{D}^*(\mathfrak{M}) \leqq T' T \bar{D}^*(\mathfrak{N}'). \tag{68}$$

Ist für alle Elemente von $\mathfrak{N}'$ auch noch die Abschätzung

$$\max_{\varkappa=S+1}^{k} \alpha_\varkappa > 1 \tag{69}$$

gültig, so folgt aus (62) sogleich

$$\bar{D}^*(\mathfrak{M}) \leqq T' \frac{12}{\pi^2} \frac{1}{S \log S}, \tag{70}$$

wobei wir ähnlich wie beim Beweis von Satz 8 schließen und die Abschätzung (66) benutzen. Für $\sigma_r(n)$ und $r > 0$ gilt

$$\sigma_r(n) = \prod_{\varkappa=1}^{k} (1 + p_\varkappa^r + p_\varkappa^{2r} + \cdots + p_\varkappa^{\alpha_\varkappa r}) \geqq n \frac{p_1 + 1}{p_1}. \tag{71}$$

Also sind die vorangehenden Sätze alle gültig, wenn wir $f(n) = \sigma_r(n)$ $(r > 0)$ und $u = 1$ setzen.

Für den Sonderfall der befreundeten Zahlen, also den Fall $f(n) = \sigma(n)$, in dem wir die Bedingungen

$$\sigma(m_1) = \sigma(m_2); \quad m_1 = \sigma(m_2) - m_2 \tag{72}$$

haben, beweisen wir zum Schluß den

Satz 13. *Es sei $\mathfrak{M}$ die Menge, die aus alle den befreundeten Zahlenpaaren m_1, m_2 besteht, bei denen wenigstens eine der beiden Zahlen m_1, m_2 nicht mehr als S verschiedene Primteiler besitzt, wobei S eine beliebig gegebene Schranke bedeutet. Dann ist $D^*(\mathfrak{M}) = 0$.*

Beweis. Wir müssen zeigen [13]), daß $\bar{D}^*(\mathfrak{M}_1) = 0$ ist, wobei $\mathfrak{M}_1$ die Menge aller $m_1 \in \mathfrak{M}$, $m_1 < m_2$ bedeutet. Wir spalten $\mathfrak{M}$ in zwei Untermengen auf: $\mathfrak{M}^{(1)}$ bestehe aus allen den Paaren m_1, m_2, bei denen $V(m_1) \leqq S$ ist; $\mathfrak{M}^{(2)}$ aus allen denen, bei welchen $V(m_1) > S$, aber wegen der Voraussetzung unseres Satzes $V(m_2) \leqq S$ ist. Weiterhin erklären wir $\mathfrak{M}_i^{(j)}$ als die Menge aller $m_i \in \mathfrak{M}^{(j)}$. Sofort sehen wir [14]), daß

$$\bar{D}^*(\mathfrak{M}_1^{(1)}) = 0 \tag{73}$$

gilt.

Nach den Sätzen 9 und 10 sowie (72) können wir von nun an voraussetzen, daß der kleinste Primteiler von jedem $m_2 \in \mathfrak{M}_2^{(2)}$ größer als eine vorgegebene Schranke $T > S^2$ ist. Dann ist

$$\frac{\sigma(m_2)}{m_2} < \frac{S^2+1}{S^2} \cdot \frac{S^2+2}{S^2+1} \cdots \frac{S^2+S}{S^2+S-1} = 1 + \frac{1}{S}. \tag{74}$$

Aus (72) und (74) folgt somit

$$\frac{m_2}{m_1} > S; \quad \frac{\sigma(m_1)}{m_1} > S + 1. \tag{75}$$

Für hinreichend große S ist dann auch $\bar{D}^*(\mathfrak{M}_1^{(2)})$ beliebig klein, also Satz 13 bewiesen. Denn bezeichnen wir mit $A_{S+1}(N)$ die Anzahl der $(S+1)$-abundanten Zahlen $\leqq N$, so ist

$$(S+1)\, A_{S+1}(N) \leqq \sum_{n \leqq N} \frac{\sigma(n)}{n} < \frac{\pi^2}{6} N; \quad \overline{\lim_{N\to\infty}} \frac{A_{S+1}(N)}{N} \leqq \frac{\pi^2}{6(S+1)}. \tag{76}$$

---

[13]) A. a. O. [1]), (28). Vgl. auch (54) der vorliegenden Arbeit.

[14]) A. a. O. [1]).

Daß die Sätze 9 und 10 knappste Voraussetzungen besitzen, erkennen wir sofort, wenn wir die Zahlen $m = \sigma(p_1 p_2) - p_1 p_2 = 1 + p_1 + p_2$ betrachten. Deren Dichte ist bekanntlich positiv. Unter Annahme der Goldbachschen Vermutung ist sie sogar gleich 0,5.

Auf ähnliche Art wie im Beweis von Satz 13 läßt sich auch zeigen, daß $D^*(\mathfrak{M}) = 0$ bereits aus $D^*(\mathfrak{M}_2) = 0$ folgt. Denn spalten wir jetzt $\mathfrak{M}$ so auf: $\mathfrak{M}^{(1)}$ bestehe genau aus den Paaren m_1, m_2, für die $\frac{m_2}{m_1} \leqq S$ ist, $\mathfrak{M}^{(2)}$ aus allen übrigen Paaren. Dann ist, wenn wir wieder mit $\mathfrak{M}_i^{(j)}$ die Menge aller $m_i \in \mathfrak{M}^{(j)}$ bezeichnen,

$$\bar{D}^*(\mathfrak{M}_1^{(1)}) \leqq S\bar{D}^*(\mathfrak{M}_2^{(1)}). \tag{77}$$

$D^*(\mathfrak{M}_2^{(1)})$ ist aber nach Voraussetzung gleich Null, weil $\mathfrak{M}_2^{(1)}$ eine Untermenge von $\mathfrak{M}_2$ ist. Für jedes $m_1 \in \mathfrak{M}_1^{(2)}$ gilt $\frac{\sigma(m_1)}{m_1} = 1 + \frac{m_2}{m_1} > S + 1$, also ist auch, wie im Beweis von Satz 13, $\bar{D}^*(\mathfrak{M}_1^{(2)})$ beliebig klein bei hinreichend großen S. Wegen

$$\bar{D}^*(\mathfrak{M}) \leqq 2\bar{D}^*(\mathfrak{M}_1) \leqq 2\sum_{i=1}^{2} \bar{D}^*(\mathfrak{M}_1^{(i)}) \tag{78}$$

folgt sogleich die Richtigkeit der obigen Behauptung. Übrigens läßt sich leicht zeigen, daß die Menge $\mathfrak{M}$ aller befreundeten Zahlenpaare die natürliche Dichte Null besitzt, wenn die Gleichungen

$$\sigma(m_1) = \sigma(m_2) = \cdots = \sigma(m_{2s-1}) = \sigma(m_{2s}) = m_1 + m_2 = m_3 + m_4 = \cdots = m_{2s-1} + m_{2s} \tag{79}$$

nicht für beliebig große s und natürliche Zahlen

$$m_1 < m_3 < \cdots < m_{2s-1} < m_{2s} < m_{2s-2} < \cdots < m_4 < m_2$$

erfüllbar sind. Das aber weiß man bisher nicht.

Zusatz bei der Korrektur. Statt Satz 2 und Satz 3 kann man mit den gleichen Methoden einen Satz beweisen, der wie Satz 2 lautet, aber an Stelle der Bedingung c) die schwächere Bedingung c) von Satz 3 hat. Einer brieflichen Mitteilung von Herrn P. Erdös (vom 19. 1. 1955) verdanke ich eine kurze Beweisskizze eines Satzes, der eine Verschärfung von Satz 13 darstellt: Für die Menge $\mathfrak{M}$ aller befreundeten Zahlenpaare ist $D^*(\mathfrak{M}) = 0$. Der Beweis dieses Satzes soll in den Publicationes Math. Debrecen erscheinen.

Eingegangen 3. Januar 1955.

Distribution of bordered symmetric, skew and hermitian matrices in a finite field.

By *L. Carlitz* and *John H. Hodges*, Durham, N. C., USA.

1. Introduction. Let $q = p^n$, $p > 2$, and let $GF(q)$ denote the finite field of order q. Let A be a non-singular symmetric matrix of order m with elements in $GF(q)$. In §§ 2, 3, 4 we consider the problem of finding the number of $m \times t$ matrices U with elements in $GF(q)$ such that the matrix

$$M = \begin{bmatrix} A & U \\ U' & 0 \end{bmatrix}, \tag{1.1}$$

where U' denotes the transpose of U, has rank $m + r$, $0 \leqq r \leqq m, t$, and invariant λ. We find (Theorem 1) that the number of solutions of this problem is equal to

$$N(t, r, \lambda')\, N_t(A, B),$$

where B is any symmetric matrix of order t, rank r and invariant λ', $N_t(A, B)$ is the number of $m \times t$ matrices V such that

$$V'AV = B,$$

$\lambda' = \psi^r(-1)\, \lambda(A)\, \lambda$, and $N(t, r, \lambda')$ is the number of symmetric matrices of order t, rank r and invariant λ'; these numbers are given explicitly by (3. 4) and (3. 6) below. In § 5 we deal with the more general case of (1. 1) in which A is of rank $s \leqq m$.

In §§ 6—9 we consider the analogous problems for skew-symmetric matrices. Finally in §§ 10—13 we treat the like problem for hermitian matrices over $GF(q^2)$.

The special problem of finding the number of M such that $\det M = \beta$ for given $\beta \in GF(q)$ has been treated for symmetric matrices in [2] and for skew matrices in [3; § 9].

2. The symmetric problem. In this section, small Greek letters $\alpha, \beta, \gamma, \ldots$ will denote elements of $GF(q)$ and italic capital letters $A, B, C, \ldots$ will denote matrices with elements in $GF(q)$, except as indicated. A' denotes the transpose of A. This notation will also be used in §§ 3, 4, 5, 6, 7, 8, 9.

If S is a symmetric matrix of order m and rank r, there exists a non-singular matrix P such that

$$P'SP = D = \operatorname{diag}(1, 1, \ldots, 1, \delta, 0, 0, \ldots, 0),$$

where the number of zeros is $m - r$. The number $\lambda(S) = \psi(\delta)$, where $\psi(\alpha) = 0, 1, -1$ according as α is zero, a square, or a non-square of $GF(q)$, is called the *invariant* of S, and D is called the normal form of S.

Let A be a fixed non-singular symmetric matrix of order m. We seek the number of $m \times t$ matrices U such that the matrix

$$M = \begin{bmatrix} A & U \\ U' & 0 \end{bmatrix} \tag{2.1}$$

has rank $m + r$, $0 \leqq r \leqq m$, t and $\lambda(M) = \lambda$; we denote this number by $\Theta_t(A, m, r, \lambda)$. If $D = \operatorname{diag}(1, 1, \ldots, \delta)$ is the normal form of A, it is clear that without loss of generality we may consider the same problem for the simpler matrix

$$M_1 = \begin{bmatrix} D & U \\ U' & 0 \end{bmatrix}. \tag{2.2}$$

Suppose that $U = (\mu_{ij})$. Then in terms of the $m + t$ variables

$$x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_t,$$

the quadratic form having matrix M_1 is

$$Q_1 = \sum_{i=1}^{m-1} x_i^2 + \delta x_m^2 + 2 \sum_{i=1}^{m} \sum_{j=1}^{t} \mu_{ij} x_i y_j. \tag{2.3}$$

Completing the square on Q_1 gives

$$\begin{aligned} Q_1 &= \sum_{i=1}^{m-1} \left\{ x_i + \sum_{j=1}^{t} \mu_{ij} y_j \right\}^2 + \delta \left\{ x_m + \delta^{-1} \sum_{j=1}^{t} \mu_{mj} y_j \right\}^2 - \sum_{i=1}^{m-1} \left(\sum_{j=1}^{t} \mu_{ij} y_j \right)^2 - \delta^{-1} \left(\sum_{j=1}^{t} \mu_{mj} y_j \right)^2 \\ &= \sum_{i=1}^{m-1} \left\{ x_i + \sum_{j=1}^{t} \mu_{ij} y_j \right\}^2 + \delta \left\{ x_m + \delta^{-1} \sum_{j=1}^{t} \mu_{mj} y_j \right\}^2 - \sum_{i=1}^{m-1} \sum_{j,k=1}^{t} \mu_{ij} \mu_{ik} y_j y_k - \delta^{-1} \sum_{j,k=1}^{t} \mu_{mj} \mu_{mk} y_j y_k. \end{aligned}$$

Under the non-singular linear transformation

$$\begin{cases} z_i = x_i + \sum_{j=1}^{t} \mu_{ij} y_j & (i = 1, 2, \ldots, m-1) \\ z_m = x_m + \delta^{-1} \sum_{j=1}^{t} \mu_{mj} y_j & \\ y_i = y_i & (i = 1, 2, \ldots, t), \end{cases} \tag{2.4}$$

the quadratic form Q_1 becomes

$$Q_2 = \sum_{i=1}^{m-1} z_i^2 + \delta z_m^2 = \sum_{i=1}^{m-1} \sum_{j,k=1}^{t} \mu_{ij} \mu_{ik} y_j y_k - \delta^{-1} \sum_{j,k=1}^{t} \mu_{mj} \mu_{mk} y_j y_k, \tag{2.5}$$

which has matrix

$$M_2 = \begin{bmatrix} D & 0 \\ 0 & -U'D^{-1}U \end{bmatrix}. \tag{2.6}$$

Since rank M = rank M_2, $\lambda(M) = \lambda(M_2)$, $\lambda(D) = \lambda(A)$, and if

$$\operatorname{rank}(-U'D^{-1}U) = \operatorname{rank}(U'AU) = k, \quad \text{then } \lambda(-U'D^{-1}U) = \psi^k(-1)\, \lambda(U'AU),$$

it follows from (2.6) that

$$\begin{aligned} \operatorname{rank} M &= m + \operatorname{rank}(U'AU) = m + k, \\ \lambda(M) &= \psi^k(-1)\, \lambda(A)\, \lambda(U'AU), \end{aligned}$$

and so $\Theta_t(A, m, r, \lambda)$ is the number of U such that

$$\begin{cases} \operatorname{rank}(U'AU) = r, \\ \lambda(U'AU) = \psi^r(-1)\, \lambda(A)\, \lambda = \lambda'. \end{cases} \tag{2.7}$$

3. A related symmetric problem. The number of $m \times t$ matrices U such that

$$U'AU = B, \tag{3.1}$$

where B is a fixed symmetric matrix of order t, rank r, and invariant λ', and A is a non-singular symmetric matrix of order m, is given in [1], where it is denoted by $N_t(A, B)$.

That this number is the same for every symmetric B of order t, rank r, and invariant λ', is evident from an examination of the following explicit formulas which give $N_t(A, B)$. By [1; Theorem 1] the number $N_r(A, B)$ of solutions of (3. 1) in the special case where $t = r$, is equal to

$$(3.\ 2)\quad \begin{cases} q^{mr-\frac{1}{2}r(r+1)}\{1-\lambda(A)\,\psi((-1)^{\frac{1}{2}m})q^{-\frac{1}{2}m}\}\{1+\lambda(A)\,\lambda'\,\psi((-1)^{\frac{1}{2}(m-r)})q^{-\frac{1}{2}(m-r)}\} \\ \qquad\qquad \cdot \prod_{i=1}^{\frac{1}{2}(r-2)}(1-q^{2i-m}) & (m \text{ even, } r \text{ even}) \\ q^{mr-\frac{1}{2}r(r+1)}\{1-\lambda(A)\,\psi((-1)^{\frac{1}{2}m})q^{-\frac{1}{2}m}\}\prod_{i=1}^{\frac{1}{2}(r-1)}(1-q^{2i-m}) & (m \text{ even, } r \text{ odd}), \\ q^{mr-\frac{1}{2}r(r+2)}\{1+\lambda(A)\,\lambda'\,\psi((-1)^{\frac{1}{2}(m-r)})q^{-\frac{1}{2}(m-r)}\} \\ \qquad\qquad \cdot \prod_{i=1}^{\frac{1}{2}(r-1)}(1-q^{2i-m-1}) & (m \text{ odd, } r \text{ odd}), \\ q^{mr-\frac{1}{2}r(r+1)}\prod_{i=1}^{\frac{1}{2}r}(1-q^{2i-m-1}) & (m \text{ odd, } r \text{ even}). \end{cases}$$

The explicit value of $N_t(A, 0)$, the number of solutions of (3. 1) with $B = 0$, is determined [1; Theorem 4] by the following relations:

$$(3.\ 3)\quad \begin{cases} q^{\frac{1}{2}t(t+1)-mt}N_t(A, 0) = 1 + \sum\limits_{1<2j\leq 2t} q^{-(m+1)j}\dfrac{\prod\limits_{i=0}^{2j-1}(1-q^{t-i})}{\prod\limits_{i=1}^{j}(1-q^{-2i})} & (m \text{ odd}), \\ q^{\frac{1}{2}t(t+1)-mt}N_t(A, 0) = 1 + \sum\limits_{1<2j\leq t} q^{-mj}\dfrac{\prod\limits_{i=0}^{2j-1}(1-q^{t-i})}{\prod\limits_{i=1}^{j}(1-q^{-2i})} \\ \qquad - q^{\frac{1}{2}m}\,\psi((-1)^{\frac{1}{2}m})\,\lambda(A)\sum\limits_{1<2j\leq t+1} q^{-mj}\dfrac{\prod\limits_{i=0}^{2j-2}(1-q^{t-i})}{\prod\limits_{i=1}^{j-1}(1-q^{-2i})} & (m \text{ even}). \end{cases}$$

Finally, by [1; Theorem 5], the number of solutions of (3. 1) in the general case is

$$(3.\ 4)\qquad N_t(A, B) = N_r(A, B^*)\,N_{t-r}(A_r, 0),$$

where A_r is symmetric of order $m-r$ and non-singular with $\lambda(A_r) = \lambda(A)\,\lambda'$, B^* is symmetric of order r and non-singular with $\lambda(B^*) = \lambda'$, and $N_r(A, B^*)$ and $N_{t-r}(A_r, 0)$ are given by (3. 2) and (3. 3) respectively.

If we specialize still further and take $m = r$, $A = B$ in (3. 1) and let

$$N_r(A, A) = E(m, \lambda'),$$

from [1; Theorem 2] the explicit value of $E(m, \lambda')$ is

$$(3.\ 5)\quad \begin{cases} 2q^{\frac{1}{2}m(m-1)}\{1-\lambda'\,\psi((-1)^{\frac{1}{2}m})q^{-\frac{1}{2}m}\}\prod_{i=1}^{\frac{1}{2}(m-2)}(1-q^{2i-m}) & (m \text{ even}), \\ 2q^{\frac{1}{2}m(m-1)}\prod_{i=1}^{\frac{1}{2}(m-1)}(1-q^{2i-m-1}) & (m \text{ odd}). \end{cases}$$

Then by [1; Theorem 3] the number of matrices of order t, rank r, and invariant λ' is

$$(3.\ 6)\qquad N(t, r, \lambda') = \frac{g_t}{q^{r(t-r)}g_{t-r}E(r, \lambda')},$$

where g_t, the number of non-singular matrices of order t, is given by the well-known formula

$$g_t = \prod_{i=0}^{t-1} (q^t - q^i) = q^{t^2} \prod_{i=1}^{t} (1 - q^{-i}). \tag{3.7}$$

4. Number of bordered symmetric matrices. Clearly the number of solutions U of (2.7) is obtained by letting B in (3.1) run through all symmetric matrices of order t, rank r and invariant λ' and summing the corresponding values of $N_t(A, B)$. Since $N_t(A, B)$ has the same value for every such B, we have

Theorem 1. *Let $\Theta_t(A, m, r, \lambda)$ denote the number of matrices M as defined in* (2.1). *Then*

$$\Theta_t(A, m, r, \lambda) = N(t, r, \lambda')\, N_t(A, B), \tag{4.1}$$

where $\lambda' = \psi^r(-1)\,\lambda(A)\,\lambda$, B is symmetric of order t, rank r and invariant λ', and $N(t, r, \lambda')$ and $N_t(A, B)$ are given by (3.6) *and* (3.4) *respectively.*

In particular for $r = t$, this result may be compared with Theorem 1 of [2]. It is not difficult to show that the results are in agreement.

5. General symmetric case. Let A be a fixed symmetric matrix of order m and rank $s \geqq 1$. Let $\Phi_t(A, m, s, r, \lambda)$ denote the number of $m \times t$ matrices U such that

$$M = \begin{bmatrix} A & U \\ U' & 0 \end{bmatrix} \tag{5.1}$$

has rank $s + r$, $r \leqq m, t$ and $\lambda(M) = \lambda$. If

$$D = \operatorname{diag}(1, 1, \ldots, \delta, 0, \ldots, 0)$$

is the normal form of A, set $D_0 = \operatorname{diag}(1, 1, \ldots, \delta)$. As in the non-singular case we may consider the question for the simpler matrix

$$M_1 = \begin{bmatrix} D & U \\ U' & 0 \end{bmatrix}. \tag{5.2}$$

With $U = (\mu_{ij})$, the quadratic form in the $m + t$ variables $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_t$ having matrix M_1 is

$$Q_1 = \sum_{i=1}^{s-1} x_i^2 + \delta x_s^2 + 2 \sum_{i=1}^{m} \sum_{j=1}^{t} \mu_{ij} x_i y_j. \tag{5.3}$$

Completing the square on Q_1 and making the non-singular linear transformation

$$\begin{cases} z_i = x_i + \sum_{j=1}^{t} \mu_{ij} y_j & (i = 1, 2, \ldots, s-1) \\ z_s = x_s + \delta^{-1} \sum_{j=1}^{t} \mu_{sj} y_j & \\ x_i = x_i & (i = s+1, \ldots, m) \\ y_i = y_i & (i = 1, 2, \ldots, t), \end{cases} \tag{5.4}$$

we find that Q_1 becomes

$$Q_2 = \sum_{i=1}^{s-1} z_i^2 + \delta z_s^2 - \sum_{i=1}^{s-1} \sum_{j,k=1}^{t} \mu_{ij} \mu_{ik} y_j y_k - \delta^{-1} \sum_{j,k=1}^{t} \mu_{sj} \mu_{sk} y_j y_k + 2 \sum_{i=s+1}^{m} \sum_{j,k=1}^{t} \mu_{ij} x_i y_j, \tag{5.5}$$

which has matrix

$$(5.6)\qquad M_2 = \begin{bmatrix} D_0 & 0 & 0 \\ 0 & 0 & U_2 \\ 0 & U_2' & -U_1' D_0^{-1} U_1 \end{bmatrix},$$

where $U_1 = (\mu_{ij})$ for $1 \leqq i \leqq s$ and $U_2 = (\mu_{ij})$ for $s+1 \leqq i \leqq m$. We may find a non-singular matrix P such that

$$(5.7)\qquad M_3 = P' M_2 P = \begin{bmatrix} D_0 & 0 & 0 \\ 0 & 0 & X_2 \\ 0 & X_2' & -X_1' D_0 X_1 \end{bmatrix} = \begin{bmatrix} D_0 & 0 \\ 0 & M_4 \end{bmatrix},$$

where rank $M_2 =$ rank M_3 and $\lambda(M_2) = \lambda(M_3)$. Since rank $M =$ rank $M_3 = s +$ rank M_4, $\lambda(A) = \lambda(D_0)$, and $\lambda = \lambda(M) = \lambda(M_3) = \lambda(A)\,\lambda(M_4)$, so that $\lambda(M_4) = \lambda(A)\,\lambda = \lambda''$, it is clear that $\Phi_t(A, m, s, r, \lambda)$ is the number of matrices M_4 having rank r and invariant λ''. Put $A_0 = -D_0$. Then if, for some X_1, rank $(X_1' A_0 X_1) = k$, with $0 \leqq k \leqq r$, the corresponding number of matrices M_4 having rank r and invariant λ'' is $\Phi_{m-s}(X_1' A_0 X_1, t, k, r-k, \lambda'')$. Thus we can write

$$(5.8)\qquad \Phi_t(A, m, s, r, \lambda) = \sum_{k=0}^{r} \sum_{\operatorname{rank}(X_1' A_0 X_1) = k} \Phi_{m-s}(X_1' A_0 X_1, t, k, r-k, \lambda'').$$

Now, as X_1 runs through all $s \times t$ matrices, if B_k is any symmetric matrix of order t and rank k, the number of X_1 in the inner sum of (5.8) for which $X_1' A_0 X_1 = B_k$ is $N_t(A_0, B_k)$. Therefore (5.8) becomes

$$(5.9)\qquad \begin{aligned} \Phi_t(A, m, s, r, \lambda) &= N_t(A_0, 0)\, \Phi_{m-s}(0, t, 0, r, \lambda'') \\ &+ \sum_{k=1}^{r} \Big\{ \sum_{\lambda(B_k)=1} N_t(A_0, B_k)\, \Phi_{m-s}(B_k, t, k, r-k, \lambda'') \\ &+ \sum_{\lambda(C_k)=-1} N_t(A_0, C_k)\, \Phi_{m-s}(C_k, t, k, r-k, \lambda'') \Big\}. \end{aligned}$$

Since $N_t(A, B)$ is the same for all B of the same order, rank and invariant and in view of (5.2) this is also true for $\Phi_{m-s}(B, t, k, r-k, \lambda'')$, (5.8) gives

Theorem 2. *Let $\Phi_t(A, m, s, r, \lambda)$ denote the number of matrices M as defined in* (5.1). *If A has normal form $D = \operatorname{diag}(1, 1, \ldots, \delta, 0, \ldots, 0)$, then*

$$(5.10)\qquad \begin{aligned} \Phi_t(A, m, s, r, \lambda) &= N_t(A_0, 0)\, \Phi_{m-s}(0, t, 0, r, \lambda'') \\ &+ \sum_{k=1}^{r} \{ N(t, k, 1)\, N_t(A_0, B_k)\, \Phi_{m-s}(B_k, t, k, r-k, \lambda'') \\ &+ N(t, k, -1)\, N_t(A_0, C_k)\, \Phi_{m-s}(C_k, t, k, r-k, \lambda'') \}, \end{aligned}$$

where $A_0 = -\operatorname{diag}(1, 1, \ldots, \delta)$, B_k and C_k are symmetric of order t and rank k, $\lambda(B_k) = +1$, $\lambda(C_k) = -1$, $\lambda'' = \lambda(A)\,\lambda$ and $N(t, k, \lambda)$, $N_t(A, 0)$ and $N_t(A, B)$ are given by (3.6), (3.3) *and* (3.4) *respectively.*

We remark that (5.10) holds for $r = 0$, $\lambda = 0$, for in this case it is necessary that $M_4 = 0$ which implies in (5.7) that $X_2 = 0$ and $X_1' A_0 X_1 = 0$. The number of such X_1, X_2, which is the value of $\Phi_t(A, m, s, 0, 0)$, is clearly $N_t(A_0, 0)$. On the other hand, for $r = 0$, $\lambda = 0$ we have $\lambda'' = 0$ and $\Phi_{m-s}(0, t, 0, 0, 0) = 1$ so that the right side of (5.10) is also equal to $N_t(A_0, 0)$. Repeated application of the recursion formula (5.10) would ultimately yield an explicit formula for $\Phi_t(A, m, s, r, \lambda)$.

As a check on Theorem 2 we may show that for $s = m$, (5. 10) reduces to (4. 1), that is,

$$\Phi_t(A, m, m, r, \lambda) = \Theta_t(A, m, r, \lambda).$$

6. The skew problem. If S is a skew-symmetric matrix of order m and rank $2r$, there exists a non-singular matrix P such that

$$(6.1) \qquad P'SP = N = \operatorname{diag}(E_1, \ldots, E_r, 0, \ldots, 0), \quad E_i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix};$$

N is called the *normal form* of S.

Let A be a fixed non-singular skew-symmetric matrix of order $2m$. We seek the number of $2m \times t$ matrices U such that the matrix

$$(6.2) \qquad M = \begin{bmatrix} A & U \\ -U' & 0 \end{bmatrix}$$

has rank $2m + 2r$, $0 \leqq 2r \leqq 2m, t$. Let $\bar{\Theta}_t(A, 2m, 2r)$ denote the number of such U. If $N = \operatorname{diag}(E_1, \ldots, E_m)$ is the normal form of A we may consider the equivalent problem for

$$(6.3) \qquad M_1 = \begin{bmatrix} N & U \\ -U' & 0 \end{bmatrix}.$$

In terms of the two sets of $2m + t$ variables $z_1, z_2, \ldots, z_{2m}, w_1, w_2, \ldots, w_t$ and $x_1, x_2, \ldots, x_{2m}, y_1, y_2, \ldots, y_t$, the bilinear form having M_1 as matrix is

$$(6.4) \qquad L_1 = \sum_{i=0}^{m-1} z_{2i+1}x_{2i+2} - \sum_{i=0}^{m-1} z_{2i+2}x_{2i+1} - \sum_{j=1}^{t}\sum_{i=1}^{2m} \mu_{ij} w_j x_i + \sum_{k=1}^{t}\sum_{i=1}^{2m} \mu_{ik} z_i y_k .$$

We may rewrite (6. 4) as

$$\begin{aligned} L_1 = & \sum_{i=0}^{m-1}\left(z_{2i+1} - \sum_{j=1}^{t}\mu_{2i+2,j}w_j\right)\left(x_{2i+2} + \sum_{k=1}^{t}\mu_{2i+1,k}y_k\right) \\ (6.5) \qquad & - \sum_{i=0}^{m-1}\left(z_{2i+2} + \sum_{j=1}^{t}\mu_{2i+1,j}w_j\right)\left(x_{2i+1} - \sum_{k=1}^{t}\mu_{2i+2,k}y_k\right) \\ & - \sum_{i=0}^{m-1}\sum_{j,k=1}^{t}\mu_{2i+2,j}\mu_{2i+1,k}w_jy_k + \sum_{i=0}^{m-1}\sum_{j,k=1}^{t}\mu_{2i+1,j}\mu_{2i+2,k}w_jy_k . \end{aligned}$$

Then under the non-singular linear transformations

$$\begin{cases} z'_{2i+1} = z_{2i+1} - \sum_{j=1}^{t}\mu_{2i+2,j}w_j & (i = 0, 1, \ldots, m-1) \\ z'_{2i+2} = z_{2i+2} + \sum_{j=1}^{t}\mu_{2i+1,j}w_j & (i = 0, 1, \ldots, m-1) \\ w_i = w_i & (i = 1, 2, \ldots, t), \end{cases}$$

and

$$\begin{cases} x'_{2i+2} = x_{2i+2} + \sum_{k=1}^{t}\mu_{2i+1,k}y_k & (i = 0, 1, \ldots, m-1) \\ x'_{2i+1} = x_{2i+1} - \sum_{k=1}^{t}\mu_{2i+2,k}y_k & (i = 0, 1, \ldots, m-1) \\ y_i = y_i & (i = 1, 2, \ldots, t), \end{cases}$$

the bilinear form becomes

$$L_2 = \sum_{i=0}^{m-1} z'_{2i+1} x'_{2i+2} - \sum_{i=0}^{m-1} z'_{2i+2} x'_{2i+1} - \sum_{i=0}^{m-1} \sum_{j,k=1}^{t} \mu_{2i+2,j} \mu_{2i+1,k} w_j y_k + \sum_{i=0}^{m-1} \sum_{j,k=1}^{t} \mu_{2i+1,j} \mu_{2i+2,k} w_j y_k, \tag{6.6}$$

which has the matrix

$$M_2 = \begin{bmatrix} N & 0 \\ 0 & U'NU \end{bmatrix} \tag{6.7}$$

(we remark that $-N^{-1} = N$). Since rank $(U'NU) =$ rank $(U'AU)$ and rank $M =$ rank M_2, it is clear from (6.7) that

$$\text{rank } M = 2m + \text{rank } (U'AU).$$

Therefore, the number of M of rank $2m + 2r$, that is $\bar{\Theta}_t(A, 2m, 2r)$, is equal to the number of U such that rank $(U'AU) = 2r$.

7. A related skew problem. The number of $m \times t$ matrices U such that

$$U'AU = B, \tag{7.1}$$

where B is a fixed skew-symmetric matrix of order t and rank $2r \leqq t$, and A is a non-singular skew-symmetric matrix of order m, is given in [3]. We denote this number here by $\bar{N}_t(A, B)$. By [3; Theorem 1] the number of solutions of (7.1) in the case $t = 2r$, that is, when B is non-singular, is

$$\bar{N}_{2r}(A, B) = q^{2rm-r^2} \prod_{i=0}^{r-1} (q^{2m-2i} - 1). \tag{7.2}$$

With $B = 0$, the number of solutions of (7.1) is $\bar{N}_t(A, 0)$ and from [3; § 3] we have the explicit formula

$$\bar{N}_t(A, 0) = q^{-\frac{1}{2}t(t-1)} \sum_{2j \leq t} q^{m(2t-j)-2j} \frac{\prod_{i=0}^{2j-1} (1 - q^{t-i})}{\prod_{i=1}^{j} (1 - q^{-2i})}. \tag{7.3}$$

Finally, by [3; Theorem 5], the number of solutions of (7.1) is

$$\bar{N}_t(A, B) = \bar{N}_{2r}(A, B^*)\, \bar{N}_{t-r}(A_{2r}, 0), \tag{7.4}$$

where A_r is skew-symmetric and non-singular of order $2m - 2r$ and

$$B^* = \text{diag}\,(E_1, E_2, \ldots, E_r), \quad E_i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

and $\bar{N}_{2r}(A, B^*)$ and $\bar{N}_{t-2r}(A_r, 0)$ are given by (7.4) and (7.3) respectively.

Furthermore by [3; Theorem 3], the number of skew-symmetric matrices of order m and rank $2r$ is

$$\bar{N}(m, 2r) = q^{r(r-1)} \frac{\prod_{i=0}^{2r-1} (q^{m-i} - 1)}{\prod_{i=1}^{r} (q^{2i} - 1)}. \tag{7.5}$$

8. Number of bordered skew-symmetric matrices. Since in § 6 we found that $\bar{\Theta}_t(A, 2m, 2r)$ is equal to the number of U such that rank $(U'AU) = 2r$, if we let B in (7. 1) run through all skew-symmetric matrices of order t and rank $2r$ and sum the corresponding values of $\bar{N}_t(A, B)$, the result is equal to $\bar{\Theta}_t(A, 2m, 2r)$. Since by (7. 4), (7. 3) and (7. 2) it is clear that $\bar{N}_t(A, B)$ depends only upon the order and rank of B, we can state

Theorem 3. *Let $\bar{\Theta}_t(A, 2m, 2r)$ denote the number of matrices M as defined in* (6. 2). *Then*

$$\bar{\Theta}_t(A, 2m, 2r) = \bar{N}(t, 2r)\, \bar{N}_t(A, B), \tag{8. 1}$$

where B is skew-symmetric of order t and rank $2r$ and $N(t, 2r)$ and $\bar{N}_t(A, B)$ are given by (7. 5) *and* (7. 4) *respectively.*

In particular for $t = 2r$, this result may be compared with Theorem 6 of [3].

9. General skew-symmetric case. Let A be a fixed skew-symmetric matrix of order m and rank $2s \geqq 2$. Let $\bar{\Phi}_t(A, m, 2s, 2r)$ denote the number of $m \times t$ matrices U such that

$$M = \begin{bmatrix} A & U \\ -U' & 0 \end{bmatrix} \tag{9. 1}$$

has rank $2s + 2r$, $0 \leqq 2r \leqq m, t$. If $N = \operatorname{diag}(E_1, E_2, \ldots, E_s, 0, \ldots, 0)$ is the normal form of A, let $A_0 = \operatorname{diag}(E_1, E_2, \ldots, E_s)$. Then by a slight variation in the argument used in §§ 6, 8 we obtain the analog, for skew-symmetric matrices, of Theorem 2, namely

Theorem 4. *Let $\bar{\Phi}_t(A, m, 2s, 2r)$ denote the number of matrices M as defined in* (9. 1). *If A has normal form $N = \operatorname{diag}(E_1, \ldots, E_s, 0, \ldots, 0)$, then*

$$\begin{aligned} \bar{\Phi}_t(A, m, 2s, 2r) &= \bar{N}_t(A_0, 0)\, g(m - 2s, t, r) \\ &\quad + \sum_{k=1}^{r} \bar{N}(t, 2k)\, \bar{N}_t(A_0, B_k)\, \bar{\Phi}_{m-2s}(B_k, t, 2k, 2r - 2k), \end{aligned} \tag{9. 2}$$

where $A_0 = \operatorname{diag}(E_1, E_2, \ldots, E_s)$, B_k is skew-symmetric of order t and rank $2k$, and $g(m - 2s, t, r)$, $\bar{N}(t, 2k)$, $\bar{N}_t(A_0, B_k)$ are given by (5. 12), (7. 5), (7. 4) *respectively.*

Repeated application of the recursion formula (9. 2) ultimately yields an explicit formula for $\bar{\Phi}_t(A, m, 2s, 2r)$. We note that (9. 2) holds for the trivial case $r = 0$ and that for $2s = m$ it reduces to (8. 1), that is

$$\bar{\Phi}_t(A, 2s, 2s, 2r) = \bar{\Theta}_t(A, 2s, 2r).$$

10. The hermitian problem. Let $q = p^n$, $p > 2$ and suppose that

$$\Theta \in GF(q^2), \quad \Theta^2 = v \in GF(q) \text{ but } \Theta \notin GF(q). \tag{10. 1}$$

Then $\alpha = a + b\Theta \in GF(q^2)$ if $a, b \in GF(q)$. The element $\bar{\alpha} = a - b\Theta$ will denote the *conjugate* of α. If $A = (\alpha_{ij})$, $\alpha_{ij} \in GF(q^2)$, is a square matrix let $A^* = \bar{A}' = (\bar{\alpha}_{ij})$ where the prime denotes transpose. Then A is said to be *hermitian* if and only if $A^* = A$.

In this section, as well as in §§ 11, 12, 13, small Greek letters $\alpha, \beta, \gamma, \ldots$ will denote elements of $GF(q^2)$ and Roman capital letters $A, B, C, \ldots$ will denote matrices with elements in $GF(q^2)$, except as indicated. If H is a hermitian matrix of order m and rank r, there exists a non-singular matrix T such that

$$T^* H T = D = \operatorname{diag}(1, 1, \ldots, 1, 0, \ldots, 0).$$

D is called the *normal form* of H.

We wish to find the number of $m \times t$ matrices U such that the matrix

$$M = \begin{bmatrix} A & U \\ U^* & 0 \end{bmatrix} \tag{10.2}$$

has rank $m + r$, $0 \leqq r \leqq m, t$, where A is a non-singular hermitian matrix of order m. Denote this number by $\Theta_t^*(A, m, r)$. Without loss of generality, A may be replaced in (10.2) by I_m, the identity of order m.

Let $U = (\mu_{ij})$. Then in terms of the $m + t$ variables $x_1, \ldots, x_m, y_1, \ldots, y_t$ the hermitian form having matrix M is

$$\begin{aligned} H &= \sum_{i=1}^{m} x_i \bar{x}_i + \sum_{i=1}^{m} \sum_{j=1}^{t} \mu_{ij} \bar{x}_i y_j + \sum_{i=1}^{m} \sum_{j=1}^{t} \bar{\mu}_{ij} x_i \bar{y}_j. \\ &= \sum_{i=1}^{m} \left\{ x_i + \sum_{j=1}^{t} \mu_{ij} y_j \right\} \left\{ \bar{x}_i + \sum_{j=1}^{t} \bar{\mu}_{ij} \bar{y}_j \right\} - \sum_{i=1}^{m} \sum_{j=1}^{t} \mu_{ij} y_j \sum_{k=1}^{t} \bar{\mu}_{ik} \bar{y}_k. \end{aligned} \tag{10.3}$$

Under the nonsingular linear transformation

$$\begin{cases} z_i = x_i + \sum_{j=1}^{t} \mu_{ij} y_j & (i = 1, 2, \ldots, m) \\ y_i = y_i & (i = 1, 2, \ldots, t), \end{cases} \tag{10.4}$$

the hermitian form H becomes

$$H_1 = \sum_{i=1}^{m} z_i \bar{z}_i - \sum_{i=1}^{m} \sum_{j,k=1}^{t} \mu_{ij} \bar{\mu}_{ik} y_j \bar{y}_k, \tag{10.5}$$

which has matrix

$$M_1 = \begin{bmatrix} I_m & 0 \\ 0 & -U^*U \end{bmatrix}. \tag{10.6}$$

Since rank $M =$ rank M_1 and rank $(U^*AU) =$ rank $(-U^*U)$, it is clear that rank $M = m +$ rank (U^*AU), and so $\Theta_t^*(A, m, r)$ is the number of U such that rank $(U^*AU) = r$.

11. A related hermitian problem. The number of $m \times t$ matrices U such that

$$U^*AU = B, \tag{11.1}$$

where B is a fixed hermitian matrix of order t and rank r and A is a non-singular hermitian matrix of order m is given in [4]. We will denote this number by $N_t^*(A, B)$. The following formulas give $N_t^*(A, B)$ explicitly. First, from [4; Theorem 3], the number of hermitian matrices of order t and rank r is

$$N^*(t, r) = q^{\frac{1}{2}r(r-1)} \prod_{i=1}^{r} \frac{(q^{2m-2(r-i)} - 1)}{(q^i - (-1)^i)}. \tag{11.2}$$

The number $N_t^*(A, 0)$ of solutions of (11.1) when $B = 0$ satisfies the relation [4; Theorem 4]

$$q^m N_t^*(A, 0) = q^{2mt} + \sum_{r=1}^{t} (-1)^{rm} q^{(2t-r)} N^*(t, r). \tag{11.3}$$

Finally by [4; Theorem 1] we have

$$N_t^*(A, B) = \prod_{i=1}^{r} (q^{2m-2i+1} + (-q)^{m-i}) N_{t-r}^*(A_r, 0), \tag{11.4}$$

where A_r is a non-singular hermitian matrix of order $m - r$.

12. Number of bordered hermitian matrices. Since we found in § 10 that $\Theta_t^*(A, m, r)$ is equal to the number of U such that rank $(U^*AU) = r$, we may obtain $\Theta_t^*(A, m, r)$ by letting B in (11. 1) run through all hermitian matrices of order t and rank r and summing the corresponding values of $N_t^*(A, B)$. Since $N_t^*(A, B)$ is the same for every such B, we have

Theorem 5. *Let $\Theta_t^*(A, m, r)$ denote the number of matrices M as defined in* (10. 2). *Then*

$$\Theta_t^*(A, m, r) = N^*(t, r)\, N_t^*(A, B), \tag{12. 1}$$

where B is hermitian of order t and rank r and $N^*(t, r)$ and $N_t^*(A, B)$ are given by (11. 2) *and* (11. 4) *respectively.*

13. General hermitian case. Let A be a fixed hermitian matrix of order m and rank $s \geqq 1$. Let $\Phi_t^*(A, m, s, r)$ denote the number of $m \times t$ matrices U such that

$$M = \begin{bmatrix} A & U \\ U^* & 0 \end{bmatrix} \tag{13. 1}$$

has rank $s + r$, $0 \leqq r \leqq m, t$. By a variation of the argument employed in §§ 11, 12 we obtain

Theorem 6. *Let $\Phi_t^*(A, m, s, r)$ denote the number of matrices M as defined in* (13. 1). *Then*

$$\begin{aligned} \Phi_t^*(A, m, s, r) &= N_t^*(I_s, 0)\, \Phi_{m-s}^*(0, t, 0, r) \\ &\quad + \sum_{k=1}^{r} N^*(t, k)\, N_t^*(I_s, B_k)\, \Phi_{m-s}^*(B_k, t, k, r-k), \end{aligned} \tag{13. 2}$$

where I_s is the identity of order s, B_k is hermitian of order t and rank k, and $N^*(t, k)$, $N_t^*(I_s, 0)$ and $N_t^*(I_s, B_k)$ are given by (11. 2), (11. 3) *and* (11. 4) *respectively.*

Repeated application of the recursion formula (13. 2) would ultimately yield an explicit formula for $\Phi_t^*(A, m, s, r)$. We remark that (13. 2) holds for $r = 0$, and reduces for $s = m$ to (12. 1), that is,

$$\Phi_t^*(A, m, m, r) = \Theta_t^*(A, m, r).$$

References.

1. *L. Carlitz*, Representations by quadratic forms in a finite field, Duke Mathematical Journal **21** (1954), pp. 123—137.
2. *L. Carlitz*, A problem involving quadratic forms in a finite field, Mathematische Nachrichten **11** (1954), pp. 135—142.
3. *L. Carlitz*, Representations by skew forms in a finite field, Archiv der Mathematik **5** (1954), pp. 19—31.
4. *L. Carlitz* and *J. H. Hodges*, Representations by hermitian forms in a finite field, Duke Mathematical Journal **22** (1955), pp. 393—405.

Duke University, Durham, N. C., U. S. A.

Eingegangen 3. Februar 1955.

Primzahldifferenzen*).

Von *Walter Knödel* in Wien.

1. Einleitung. P. Erdös und A. Rényi haben 1949 die Abschätzung

$$c_1 \frac{x}{\log^2 x} < \sum_{p_n < x} \frac{1}{d_n} < c_2 \frac{x}{\log^2 x} \log\log x \tag{1}$$

gegeben [1]. Dabei ist p_n die n-te Primzahl ($p_0 = 2$) und $d_n = p_n - p_{n-1}$ für $n \geqq 1$; die c_i sind positive Konstante. Schmetterer und ich haben 1951 bemerkt, daß

$$\sum_{p_n < x} \left| \frac{1}{d_n} - \frac{1}{d_{n+1}} \right|$$

zwischen den gleichen Größenordnungen liegt, deß also

$$c_3 \frac{x}{\log^2 x} < \sum_{p_n < x} \left| \frac{1}{d_n} - \frac{1}{d_{n+1}} \right| < c_4 \frac{x}{\log^2 x} \log\log x \tag{2}$$

gilt; doch haben wir das Resultat nicht veröffentlicht. Im folgenden soll gezeigt werden:

Satz 1. *Die Summen*

$$S_1(x) = \sum_{p_n < x} \frac{1}{d_n}$$

und

$$S_2(x) = \sum_{p_n < x} \left| \frac{1}{d_n} - \frac{1}{d_{n+1}} \right|$$

besitzen die gleiche Größenordnung:

$$c_5 \sum_{p_n < x} \frac{1}{d_n} < \sum_{p_n < x} \left| \frac{1}{d_n} - \frac{1}{d_{n+1}} \right| < c_6 \sum_{p_n < x} \frac{1}{d_n}. \tag{3}$$

Die Beweise sind elementar und verwenden die Methode von Brun. Dabei ergibt sich als Nebenresultat

Satz 2. *Die wahre Größenordnung von*

$$\sum_{p_n < x}' \frac{1}{d_n},$$

wobei der Strich am Summenzeichen Summation über alle $d_n \geqq d_{n-1}$, $n \geqq 2$ *bedeutet, ist*

$$c_7 \frac{x}{\log^2 x} < \sum_{p_n < x}' \frac{1}{d_n} < c_8 \frac{x}{\log^2 x}.$$

*) Vorgetragen auf der Spezialtagung für Zahlentheorie, Mathematisches Forschungsinstitut Oberwolfach, 3.—8. Januar 1955.

2. Beweis von Satz 1. Wir zeigen zunächst

$$\sum_{p_n<x}\left|\frac{1}{d_n}-\frac{1}{d_{n+1}}\right| < c_6 \sum_{p_n<x}\frac{1}{d_n}.$$

Offenbar ist

$$\sum_{p_n<x}\left|\frac{1}{d_n}-\frac{1}{d_{n+1}}\right| \leqq \sum_{p_n<x}\left\{\left|\frac{1}{d_n}\right|+\left|\frac{1}{d_{n+1}}\right|\right\}$$

$$< 2\sum_{\substack{p_n<x\\ p_{k+1}>x\\ p_k<x}}\frac{1}{d_n}+\frac{1}{d_{n+1}} \leqq 2\sum_{p_n<x}\frac{1}{d_n}+\frac{1}{2}$$

$$< c_6 \sum_{p_n<x}\frac{1}{d_n}.$$

Sodann soll gezeigt werden:

$$c_5 \sum_{p_n<x}\frac{1}{d_n} < \sum_{p_n<x}\left|\frac{1}{d_n}-\frac{1}{d_{n+1}}\right|. \tag{4}$$

Hierzu werden wir in Nr. 3 bis 8

$$D(x) = S_1(x) - S_2(x) < c_9 \frac{x}{\log^2 x} \tag{5}$$

beweisen. Daraus folgt nach Division durch $S_1(x)$

$$1 - \frac{c_9 \dfrac{x}{\log^2 x}}{S_1(x)} < \frac{S_2(x)}{S_1(x)}, \tag{6}$$

und hiermit ergibt sich die Ungleichung (4) mit der Fallunterscheidung

a) für jene x, für die

$$S_1(x) > c_{10}\frac{x}{\log^2 x},$$

b) für jene x, für die

$$S_1(x) \leqq c_{10}\frac{x}{\log^2 x}$$

ist, wobei $c_{10} > c_9$ sein soll. Denn im Fall a) gilt

$$1 - \frac{c_9 \dfrac{x}{\log x}}{S_1(x)} > 1 - \frac{c_9}{c_{10}}$$

und nach (6)

$$S_1\left(1-\frac{c_9}{c_{10}}\right) < S_2.$$

Im Fall b) folgern wir aus (2)

$$\frac{c_3}{c_{10}} S_1 < S_2.$$

Mit

$$c_5 = \operatorname{Min}\left(\frac{c_3}{c_{10}}, 1-\frac{c_9}{c_{10}}\right)$$

folgt also (4).

3. Abschätzung von D(x). Wir zerlegen

$$(7) \qquad D(x) = \sum_{p_n < x} \left\{ \frac{1}{d_n} - \left| \frac{1}{d_n} - \frac{1}{d_{n+1}} \right| \right\} = D_1(x) + D_2(x) + D_3(x).$$

Hierbei soll $D_1(x)$ jene Bestandteile von (7) enthalten, für die

$$(8) \qquad d_n \leqq d_{n+1},$$

$D_2(x)$ jene Bestandteile von (7), für die

$$(9) \qquad d_{n+1} < d_n \leqq 2d_{n+1},$$

$D_3(x)$ jene Bestandteile von (7), für die

$$(10) \qquad 2d_{n+1} < d_n$$

ist. Nun zeigen wir: $D_3(x) < 0$. Nach Definition gilt

$$D_3(x) = \sum_{\substack{p_n < x \\ 2d_{n+1} < d_n}} \left\{ \frac{1}{d_n} - \left| \frac{1}{d_n} - \frac{1}{d_{n+1}} \right| \right\}$$

und wegen (10)

$$\frac{1}{d_n} < \frac{1}{d_{n+1}}.$$

Daher haben wir

$$D_3(x) = \sum_{\substack{p_n < x \\ 2d_{n+1} < d_n}} \left\{ \frac{1}{d_n} - (-1)\left(\frac{1}{d_n} - \frac{1}{d_{n+1}} \right) \right\} = \sum_{\substack{p_n < x \\ 2d_{n+1} < d_n}} \left\{ \frac{2}{d_n} - \frac{1}{d_{n+1}} \right\}.$$

Hierin ist wieder nach (10) jede geschweifte Klammer negativ und daher auch die ganze Summe D_3 $\left(\text{die sicher nicht leer ist, denn sie enthält z. B. das Glied } \frac{2}{29-23} - \frac{1}{31-29}\right)$. Daraus folgt weiter

$$D(x) < D_1(x) + D_2(x),$$

und für den Beweis von (5) genügt es,

$$(11) \qquad D_1(x) < c_{11} \frac{x}{\log^2 x}$$

$$(12) \qquad D_2(x) < c_{12} \frac{x}{\log^2 x}$$

zu zeigen, wobei wir für c_9 in (5) die Konstante $c_{11} + c_{12}$ nehmen können.

4. Hilfssätze. Dem Beweis der Formeln (11) und (12) müssen wir zunächst einige Hilfssätze vorausschicken.

Hilfssatz 1. *Bezeichnen wir die Anzahl der Primzahltripel p_{k-1}, p_k, p_{k+1}, die den Bedingungen*

$$p_k - p_{k-1} = a, \quad p_{k+1} - p_k = b, \quad p_k < x$$

genügen, mit

$$\pi(x, a, b) \left\{ = \sum_{\substack{d_{k+1}=b \\ d_k=a \\ p_n<x}} 1 \right\}, \tag{13}$$

dann gilt

$$\pi(x, a, b) < c_{13} \frac{x}{\log^3 x} \sum_{d|ab(a+b)} \frac{c_{14}^{v(d)}}{d}.$$

Dabei bedeutet $v(d)$ die Anzahl der verschiedenen Primteiler von d, überdies brauchen für d nur quadratfreie Zahlen genommen zu werden.

Beweis. Aus [2], Satz 2 entnimmt man

$$\pi(x, a, b) < c_{15}\, c(a, b) \frac{x}{\log^3 x} + 3 \tag{14}$$

und für $c(a, b)$ finden wir in [2], S. 73

$$c(a, b) < \prod_{d|ab(a+b)} \left(1 - \frac{1}{p}\right)^{-3}. \tag{15}$$

Ferner wird in [3], S. 140 gezeigt, daß sich (15) mit

$$\prod_{p|ab(a+b)} \left(1 - \frac{1}{p}\right)^{-3} < \sum_{d|ab(a+b)} \frac{c_{14}^{v(d)}}{d}, \tag{16}$$

d quadratfrei, abschätzen läßt. (14), (15) und (16) liefern das gewünschte Ergebnis.

Hilfssatz 2. $\sum_d \frac{c_{15}^{v(d)}}{d^2} < c_{16}$.

Der Beweis ist bekannt (man vergleiche z. B. [4], S. 888) und kann durch Umformen des Produkts

$$\prod_p \left(1 + \frac{c_{15}}{p^2}\right)$$

geführt werden.

Schon jetzt stellen wir noch ein Ergebnis für den Beweis von Satz 2 bereit, das die Anzahl der $d_n \geqq d_{n-1}$ betrifft:

Hilfssatz 3. $\sum_{\substack{d_n \geq d_{n-1} \\ p_n<x}} 1 > c_{17} \frac{x}{\log x}$.

Beweis. Man benutze Theorem 1 von [4] und den Primzahlsatz.

5. Beweis von (11). Aus der Definition (8) von $D_1(x)$ folgt

$$\begin{aligned} D_1(x) &= \sum_{\substack{p_n<x \\ d_n \leq d_{n+1}}} \left\{ \frac{1}{d_n} - \left| \frac{1}{d_n} - \frac{1}{d_{n+1}} \right| \right\} \\ &= \sum_{\substack{p_n<x \\ d_n \leq d_{n+1}}} \left\{ \frac{1}{d_n} - \left(\frac{1}{d_n} - \frac{1}{d_{n+1}} \right) \right\} \\ &= \sum_{\substack{p_n<x \\ d_n \leq d_{n+1}}} \frac{1}{d_{n+1}} \end{aligned} \tag{17}$$

Diese Summe teilen wir weiter in $D_1(x) = D_{11}(x) + D_{12}(x)$ mit

$$D_{11}(x) = \sum_{\substack{p_n < x \\ d_n \leq d_{n+1} \\ d_{n+1} \geq c_{15} \log x}} \frac{1}{d_{n+1}} \tag{18}$$

und

$$D_{12}(x) = \sum_{\substack{p_n < x \\ d_n \leq d_{n+1} \\ d_{n+1} < c_{15} \log x}} \frac{1}{d_{n+1}} \tag{19}$$

und zeigen

$$D_{11}(x) < c_{19} \frac{x}{\log^2 x} \tag{20}$$

$$D_{12}(x) < c_{20} \frac{x}{\log^2 x}. \tag{21}$$

Daraus folgt (11) mit $c_{11} = c_{19} + c_{20}$.

6. Beweis von (20). Nach bekannten Sätzen gilt für die Anzahl der Primzahlen kleiner als x

$$\pi(x) = \sum_{p_n < x} 1 < c_{21} \frac{x}{\log x}.$$

Daher können wir (18) so abschätzen:

$$D_{11}(x) = \frac{1}{c_{18} \log x} \sum_{p_n < x} 1 = \frac{c_{21}}{c_{18}} \frac{x}{\log^2 x}.$$

Damit ist (20) mit

$$c_{19} = \frac{c_{21}}{c_{18}}$$

bewiesen.

7. Beweis von (21). Wir formen (19) zu

$$D_{12}(x) = \sum_{b < c_{15} \log x} \frac{1}{b} \sum_{\substack{d_{n+1} = b \\ d_n \leq b \\ p_n < x}} 1$$

um. Das läßt sich auch schreiben als

$$D_{12}(x) = \sum_{b < c_{15} \log x} \frac{1}{b} \cdot \sum_{a \leq b} \sum_{\substack{d_{n+1} = b \\ d_n = a \\ p_n < x}} 1,$$

oder mit (13)

$$D_{12}(x) = \sum_{b < c_{15} \log x} \frac{1}{b} \sum_{a \leq b} \pi(x, a, b).$$

Somit liefert Hilfssatz 1

$$D_{12}(x) < c_{13} \frac{x}{\log^3 x} \sum_{b < c_{15} \log x} \frac{1}{b} \sum_{a \leq b} \sum_{d \mid ab(a+b)} \frac{c_{14}^{\nu(d)}}{d}.$$

Was wir noch zu zeigen haben, ist daher

$$E = \sum_{b < c_{15} \log x} \frac{1}{b} \sum_{a \leq b} \sum_{d \mid ab(a+b)} \frac{c_{14}^{\nu(d)}}{d} \leq c_{22} \log x. \tag{22}$$

Wir schätzen E durch Vertauschen der Summationsfolge ab:

$$E = \sum_d \frac{c_{14}^{\nu(d)}}{d} \sum_{b < c_{18} \log x} \frac{1}{b} \sum_{\substack{a \leq b \\ d \mid ab(a+b)}} 1.$$

Diese Summe unterteilen wir weiter in

$$E = \sum_d \frac{c_{14}^{\nu(d)}}{d} \sum_t \sum_{\substack{b < c_{18} \log x \\ (d,b)=t}} \frac{1}{b} \sum_{\substack{a \leq b \\ \frac{d}{t} \mid a(a+b)}} 1. \tag{23}$$

Um die letzte Summe abschätzen zu können, müssen wir zuerst die Lösungszahl der Kongruenz

$$x(x+b) \equiv 0 \pmod{\frac{d}{t}} \tag{24}$$

feststellen. Wir beginnen mit der einfacheren Kongruenz

$$x(x+b) \equiv 0 \pmod{p_i}, \quad (p_i, b) = 1.$$

Diese Kongruenz besitzt genau 2 mod p_i inkongruente Lösungen. Nun erinnern wir uns, daß d $\left(\text{und daher auch } \frac{d}{t}\right)$ quadratfrei ist und $\frac{d}{t}$ daher eine Primzahlzerlegung der Form

$$\frac{d}{t} = \prod_{k \leq \nu\left(\frac{d}{t}\right)} p_{i_k}, \qquad (p_{i_k}, b_i) = 1$$

besitzt. Nach bekannten Sätzen der elementaren Zahlentheorie besitzt daher die Kongruenz (24) genau

$$2^{\nu\left(\frac{d}{t}\right)}$$

mod $\frac{d}{t}$ inkongruente Lösungen. Daraus gewinnen wir die Formel

$$\sum_{\substack{a \leq b \\ \frac{d}{t} \mid a(a+b)}} 1 \leq \left(\frac{b}{\frac{d}{t}} + 1\right) 2^{\nu\left(\frac{d}{t}\right)} < c_{23}\, 2^{\nu\left(\frac{d}{t}\right)} \frac{tb}{d},$$

und mit ihrer Hilfe erhalten wir aus (23) die Gleichung

$$E < \sum_d \frac{c_{14}^{\nu(d)}}{d} \sum_t \sum_{\substack{b < c_{18} \log x \\ (d,b)=t}} \frac{1}{b} c_{23}\, 2^{\nu\left(\frac{d}{t}\right)} \frac{tb}{d}$$

also

$$\begin{aligned} E &< c_{23} \sum_d \frac{c_{24}^{\nu(d)}}{d^2} \sum_t t \sum_{\substack{b < c_{18} \log x \\ (d,b)=t}} 1 \\ &\leq c_{23} \sum_d \frac{c_{24}^{\nu(d)}}{d_2} \sum_{t \mid d} t \sum_{\substack{b < c_{18} \log x \\ t \mid b}} 1 \\ &< c_{25} \sum_d \frac{c_{24}^{\nu(d)}}{d^2} \sum_{t \mid d} t \frac{\log x}{t} \\ &= c_{25} \log x \sum_d \frac{c_{24}^{\nu(d)}}{d^2} \sum_{t \mid d} 1 \\ &= c_{25} \log x \sum_d \frac{c_{24}^{\nu(d)} 2^{\nu(d)}}{d^2}, \end{aligned}$$

und aus Hilfssatz 2 folgt (22). Damit ist auch (11) vollständig bewiesen.

8. Beweis von (12). Der Beweis von (12) kann Schritt für Schritt genau so geführt werden wie der von (11). Wir wollen nur die wesentlichen Punkte hervorheben: An die Stelle von (17) tritt nun wegen (9)

$$D_2(x) = \sum_{\substack{p_n<x \\ d_{n+1}<d_n\leq 2d_{n+1}}} \left\{\frac{1}{d_n} - \left|\frac{1}{d_n} - \frac{1}{d_{n+1}}\right|\right\}$$

$$= \sum_{\substack{p_n<x \\ d_{n+1}<d_n\leq 2d_{n+1}}} \left\{\frac{2}{d_n} - \frac{1}{d_{n+1}}\right\} \leqq 2 \sum_{\substack{p_n<x \\ d_n>d_{n+1}}} \frac{1}{d_n}.$$

Der Unterschied gegen (11) besteht also in folgendem: (11) war die Summe über jene reziproken Differenzen, die größer waren als die vorhergehenden. (12) ist kleiner als die Summe jener reziproken Differenzen, die größer sind als die nachfolgenden. Schreibt man wieder b für die größere, a für die kleinere Differenz, dann lassen sich alle Beweise sofort wie bei (11) führen, da sie im wesentlichen auf Hilfssatz 1 beruhen und dieser für $\pi(x, a, b)$ und $\pi(x, b, a)$ dieselbe Schranke liefert.

9. Beweis von Satz 2. Ersetzt man $n + 1$ in (17) durch n, dann erhält man aus (11)

$$\sum_{\substack{p_{n-1}<x \\ d_{n-1}\leq d_n}} \frac{1}{d_n} < c_{11} \frac{x}{\log^2 x}.$$

Daher gilt um so mehr

$$\sum_{\substack{p_n<x \\ d_{n-1}\leq d_n}} \frac{1}{d_n} < c_{11} \frac{x}{\log^2 x},$$

und die rechte Seite von Satz 2 ist bewiesen.

Der Beweis der linken Seite erfolgt so: Nach Hilfssatz 3 stehen uns mehr als

$$c_{17} \frac{x}{\log x} \tag{25}$$

Differenzen $d_n \geqq d_{n-1}$ zur Verfügung. Ferner ist $p_n < x$ gleichbedeutend mit

$$\sum_{p_n<x} d_n < x. \tag{26}$$

Aus (26) erkennen wir, daß die Anzahl der großen Differenzen klein ist:

$$x > \sum_{p_n<x} d_n \geqq \sum_{\substack{p_n<x \\ d_n>\frac{2}{c_{17}}\log x}} d_n \geqq \frac{2}{c_{17}} \log x \sum_{\substack{p_n<x \\ d_n>\frac{2}{c_{17}}\log x}} 1$$

oder

$$\sum_{\substack{p_n<x \\ d_n>\frac{2}{c_{17}}\log x}} 1 < \frac{c_{17}}{2} \frac{x}{\log x},$$

und diese Schranke besteht um so mehr für

$$\sum_{\substack{p_n<x \\ d_n>\frac{2}{c_{17}}\log x \\ d_n\geq d_{n-1}}} 1.$$

Dann gilt nach (25)

$$\sum_{\substack{p_n < x \\ d_n \leq \frac{2}{c_{17}} \log x \\ d_n \geq d_{n-1}}} 1 > \frac{c_{17}}{2} \frac{x}{\log x} \tag{27}$$

und weiter

$$\sum_{\substack{d_n \geq d_{n-1} \\ p_n < x}} \frac{1}{d_n} \geqq \sum_{\substack{d_n \geq d_{n-1} \\ p_n < x \\ d_n \leq \frac{2}{c_{17}} \log x}} \frac{1}{d_n} \geqq \frac{1}{\frac{2}{c_{17}} \log x} \sum_{\substack{d_n \geq d_{n-1} \\ p_n < x \\ d_n \leq \frac{2}{c_{17}} \log x}} 1,$$

also endlich nach (27)

$$\sum_{\substack{d_n \geq d_{n-1} \\ p_n < x}} \frac{1}{d_n} > \frac{c_{17}}{2 \log x} \frac{c_{17}}{2} \frac{x}{\log x},$$

und auch Satz 2 ist vollständig bewiesen.

Literatur.

1] *P. Erdös* und *A. Rényi*, Some Problems and Results on Consecutive Primes. Simon Stevin **29** (1949/50), 115—125.

[2] *W. Knödel*, Sätze über Primzahlen. Monatshefte für Mathematik **55** (1951), 62—75.

[3] *W. Knödel*, Sätze über Primzahlen II. Monatshefte für Mathematik **56** (1952), 137—143.

[4] *P. Erdös*, On the Difference of Consecutive Primes. Bulletin of the Am. Math. Soc. **54** (1948), 885—889.

Eingegangen 5. Februar 1955.

Über additive zahlentheoretische Funktionen *).

Von *H. Halberstam*, Exeter.

Es werden im folgenden einige Ergebnisse in der Theorie der stark additiven zahlentheoretischen Funktionen beschrieben, und insbesondere wird der Beweis eines dieser Resultate kurz skizziert.

Eine stark additive Funktion $F(m)$ ist definiert durch die Eigenschaften

$$F(mn) = F(m) + F(n), \quad (m, n) = 1, \tag{1}$$

$$F(p^\alpha) = F(p), \quad p \text{ Primzahl}; \quad \alpha = 2, 3, \ldots \tag{2}$$

Ein wohlbekanntes Beispiel solch einer Funktion ist $\omega(m)$, die Anzahl der verschiedenen Primteiler von m. 1917 haben Hardy und Ramanujan bewiesen[1]), daß $\omega(m)$ die normale Größe $\log\log m$ hat; das heißt, daß $\omega(m)$ für fast alle m ungefähr gleich $\log\log m$ ist. 1934 gelang Turán[2]) ein sehr vereinfachter Beweis des Hardy-Ramanujan Satzes, und 1936 erweiterte er diesen Satz auf eine allgemeinere Klasse stark additiver Funktionen[3]). 1953 hat Delange[4]) mehr bewiesen, nämlich, daß die Verteilung der Werte von $\omega(m)$ in einem gewissen Sinne eine Gauss'sche Verteilung ist. Alle diese Ergebnisse kann man aus dem folgenden Satz[5]) ableiten:

Satz 1. *Sei* $A_n = \sum_{p<n} F(p)/p$, $B_n = \sum_{p<n} F^2(p)/p$ *und*

$$F(p) = O(1), \quad B_n \to \infty, \tag{3}$$

dann gilt für jedes feste $k = 1, 2, 3, \ldots$

$$\lim_{n\to\infty} \frac{\sum_{m=1}^{n} \{F(m) - A_n\}^k}{n B_n^{k/2}} = (2\pi)^{-1/2} \int_{-\infty}^{\infty} w^k e^{-\frac{1}{2}w^2} dw. \tag{4}$$

Wie Delange bemerkt hat, ist die Methode auch dann anwendbar, wenn man (3) auf

$$F(p) = o(B_p^{1/2}), \quad B_n \to \infty, \tag{5}$$

abschwächt.

---

*) Vorgetragen auf der Spezialtagung für Zahlentheorie, Mathematisches Forschungsinstitut Oberwolfach, 3.—8. Januar 1955.

[1]) *G. H. Hardy-S. Ramanujan*, Quart. J. Math. Oxford Ser. 48 (1917) 76—92.

[2]) *P. Turán*, J. London Math. Soc. 9 (1934), 274—276.

[3]) *P. Turán*, J. London Math. Soc. 11 (1936), 125—133.

[4]) *H. Delange*, C. R. Acad. Sci. Paris 237 (1953), 542—544.

[5]) *H. Halberstam*, J. London Math. Soc. 30 (1955), 43—53.

Die Formel (4) zeigt, daß in einem gewissen Sinne auch die Verteilung von $F(m)$ normal ist. Denn sei $k_n(w)$ die Anzahl der natürlichen Zahlen m, $1 \leqq m \leqq n$, für die

$$F(m) < A_n + wB_n^{1/2}$$

ist, und sei $\sigma_n(w) = k_n(w)/n$. Dann ist $\sigma_n(w)$ eine Verteilungsfunktion, und aus (4) folgt

$$\lim_{n\to\infty} \int_{-\infty}^{\infty} w^k d\sigma_n(w) = (2\pi)^{-1/2} \int_{-\infty}^{\infty} w^k e^{-w^2/2} dw, \quad k = 1, 2, 3, \ldots.$$

Eine berühmte Methode von Tchebycheff macht es nun möglich, aus diesen Gleichungen die Beziehung

$$\lim_{n\to\infty} \sigma_n(w) = (2\pi)^{-1/2} \int_{-\infty}^{w} e^{-u^2/2} du \tag{6}$$

herzuleiten. (6) wurde von Erdös und Kac [6]) mit anderen Methoden bewiesen.

Diese Untersuchungen kann man jetzt in einigen Richtungen fortsetzen. Erstens kann man fragen, was aus der Formel (4) wird, wenn $F(p)$ die in (5) angegebene Größenordnung überschreitet. Insbesondere hat Erdös die Frage aufgeworfen, was geschieht, wenn $F(p) = (\log p)^h$ ist (h eine positive Konstante). Ich kann nun beweisen, daß die durch

$$F(m) < w(\log n)^h, \quad 1 \leqq m \leqq n,$$

charakterisierte Verteilung nicht mehr normal ist. Es ist nämlich

$$\lim_{n\to\infty} \frac{\sum_{m=1}^{n} (F(m))^k}{n(\log n)^{hk}} = \frac{k!}{\Gamma(hk+1)} \sum_{s=1}^{k} \sum_{\substack{r_1+\cdots+r_s=k \\ r_1\geq\cdots\geq r_s\geq 1}} \frac{\Gamma(hr_1)\cdots\Gamma(hr_s)}{r_1!\cdots r_s!} \tau(r_1, \ldots, r_s), \quad k = 1, 2, \ldots \tag{7}$$

wobei

$$\tau(r_1, \ldots, r_s) = \sum \frac{1}{\nu_1!\cdots\nu_\sigma!} \qquad (\nu_1 r_1 + \cdots + \nu_\sigma r_\sigma = k, \ \nu_1 + \cdots + \nu_\sigma = s).$$

Daher ist es möglich zu beweisen, daß für $h = 1$ keine Verteilungsfunktion existiert, und für $h \neq 1$ eine eindeutige Verteilungsfunktion vorhanden ist. Die entsprechende Verteilung ist sicherlich nicht allgemein bekannt, und bisher ist es nur möglich, die Verteilungsfunktion implizit als Lösung einer nichtelementaren Integralgleichung anzugeben.

Eine weitere Untersuchung bezieht sich auf Polynome. Es sei $f(x)$ ein irreduzibles Polynom von beliebigem Grade mit ganzzahligen Koeffizienten. Wir nehmen einfachheitshalber an, daß $f(1), f(2), f(3), \ldots$ positiv sind und fragen nach der Verteilung der Werte der $F(f(m))$, $1 \leqq m \leqq n$. Dann gilt der folgende

Satz 2. Sei $\varrho(a)$ *die Anzahl der Lösungen von* $f(m) \equiv 0 \pmod{a}$, $0 \leqq m < a$,

$$A(n) = \sum_{p<n} F(p)\, \varrho(p)/p, \quad B(n) = \sum_{p<n} F^2(p)\, \varrho(p)/p,$$

und sei $F(p)$ *den Bedingungen*

$$F(p) = o(B^{1/2}(p)), \quad B(n) \to \infty,$$

unterworfen. Dann gilt für jedes feste $k = 1, 2, 3, \ldots$

$$\lim_{n\to\infty} \frac{\sum_{m=1}^{n} \{F(f(m)) - A(n)\}^k}{n\{B(n)\}^{k/2}} = (2\pi)^{-1/2} \int_{-\infty}^{\infty} w^k e^{-w^2/2} dw.$$

[6]) *P. Erdös-M. Kac*, Amer. J. Math. 62 (1940), 738—742.

Dieser Satz enthält Turáns Resultat[3]), daß die normale Größe von $\omega(f(m))$ auch $\log\log m$ ist. Ein ähnlicher Satz gilt auch für reduzible Polynome.

Die Beweismethode für Satz 1 ist elementar, und die Beweise der anderen obigen Resultate sind ähnlich, jedoch benutzen diese späteren Sätze nichtelementare Ergebnisse über die Funktion $\varrho(a)$.

Schließlich kann man eine andere, aber verwandte Frage erheben, nämlich die nach der Verteilung der Werte von $F(f(p))$, (p Primzahl). Erdös, Haselgrove und Prachar haben die ersten Schritte zur Beantwortung dieser Frage getan, und zwar hat Erdös[7]) 1935 bewiesen, daß $\omega(p-1)$ die normale Größe $\log\log p$ hat und auch daß

$$\sum_{p\leq n} \omega(p-1) \sim n(\log\log n)/\log n$$

ist. Ein Satz von Haselgrove[8]) besagt, daß

$$\sum_{p\leq n} \{\omega(p+a)\}^k \sim n(\log\log n)^k/\log n \quad \text{für jedes feste } k = 1, 2, 3, \ldots$$

gilt, und Prachar[9]) hat bewiesen, daß es eine positive Konstante c gibt, so daß

$$\sum_{p\leq n} \omega(f(p)) > cn\,(\log\log n)/\log n$$

ist.

Nun möchte ich noch kurz die wichtigsten Schritte zum Beweis des folgenden Satzes schildern:

Satz 3. $$\sum_{p\leq n} \omega(f(p)) = \{1 + o(1)\}\, n(\log\log n)/\log n.$$

Mit derselben Methode läßt sich auch beweisen, daß $\omega(f(p))$ die normale Größe $\log\log p$ hat. Die Verbindung eines schwierigen Satzes von Tatuzawa[10]) und der Methode, die ich beim Beweis der Sätze 1 und 2 benutzte, liefert auch den viel besseren

Satz 4. *Sei*

$$F(p) = O(1), \quad B(n) \to \infty, \quad \frac{(\log\log\log n)^3}{B(n)} \to 0.$$

Dann gilt für jedes feste $k = 1, 2, 3, \ldots$

$$\lim_{n\to\infty} \frac{\sum_{p\leq n} \{F(f(p)) - A(n)\}^k}{\pi(n)\,\{B(n)\}^{k/2}} = (2\pi)^{-1/2} \int_{-\infty}^{\infty} w^k e^{-w^2/2}\, dw.$$

Beweis von Satz 3.

Sei l der Grad von $f(x)$, $l \geqq 2$; p, q bezeichnen Primzahlen, $c_1, c_2, \ldots$ positive Konstanten, die höchstens von l und den Koeffizienten von $f(x)$ abhängen. Wir setzen

$$\mu = \log n, \quad \nu = \log\log n,$$

$$x_1 = n^{1/\sqrt{\nu}}, \quad x_2 = n^{1/\nu^2}, \quad x_3 = n^{1/2} x_1^{-1},$$

$$\omega_{x_r}(f(p)) = \sum_{\substack{q\leq x_r \\ q\,|\,f(p),\ q\,\nmid\, f(0)}} 1 \qquad (r = 1, 2),$$

so daß

$$\omega(f(p)) - \omega_{x_1}(f(p)) = \sum_{\substack{q > x_1 \\ q\,|\,f(p)}} 1 + O(1) = O(\nu^{1/2})$$

---

[7]) *P. Erdös*, Quart. J. Math. Oxford Ser. **6** (1935), 205—213.

[8]) *C. B. Haselgrove*, J. London Math. Soc. **26** (1951), 273—277.

[9]) *K. Prachar*, J. London Math. Soc. **28** (1953), 236—239.

[10]) *T. Tatuzawa*, Jap. Journ. of Math. **20** (1950), 93—111.

(denn hat die Summe t Glieder, so ist $x_1^t \leqq c_1 n^l$, also $t \leqq c_2 \nu^{1/2}$). Wir definieren

$$S(n) = \sum_{p \leqq n} \omega(f(p)), \quad S_1(n) = \sum_{p \leqq n} \omega_{x_1}(f(p)), \quad S_r^*(n) = \sum_{x_r < p \leqq n} \omega_{x_r}(f(p)) \qquad (r = 1, 2)$$

und bemerken, daß

$$S(n) = S_1(n) + O(n\mu^{-1}\nu^{1/2}), \quad S_1(n) = S_1^*(n) + O(n^{1/2})$$

ist und daher

$$S(n) = S_1^*(n) + O(n\mu^{-1}\nu^{1/2}). \tag{8}$$

Nun müssen wir tiefere Hilfsmittel heranziehen, um

$$S_1^*(n) = S_2^*(n) + O(n\mu^{-1}\log\nu) \tag{9}$$

zu beweisen. Wir schreiben

$$S_1^*(n) - S_2^*(n) = \sum_{\substack{x_2 < q \leqq x_1 \\ q \nmid f(0)}} \sum_{\substack{x_3 < p \leqq n \\ f(p) \equiv 0 \,(\mathrm{mod}\, q)}} 1 \leqq \sum_{\substack{x_2 < q \leqq x_1 \\ q \nmid f(0)}} \sum_{a} M(a, q),$$

wo a die $\varrho(q)$ Lösungen von $f(m) \equiv 0 \pmod q$, $0 \leqq m \leqq q$, durchläuft, und $M(a, q)$ die Anzahl derjenigen $m, x_3 < m \leqq n$, $m \equiv a \pmod q$ ist, die durch keine Primzahl $p < x_3$ teilbar sind. Also muß man hier eine Siebmethode einführen, und zwar habe ich A. Selbergs schöne und einfache Methode[11]) benutzt, um

$$M(a, q) \leqq c_3 \frac{n}{q} \mu^{-1}$$

zu beweisen. Es ist wohlbekannt, daß

$$\sum_{p \leqq x} \varrho(p)/p = \log\log x + c_4 + o(1)$$

ist, und damit ist (9) bewiesen. Wir können nun

$$S(n) = S_2^*(n) + O(n\mu^{-1}\nu^{1/2}) \tag{10}$$

erhalten.

Nun setzen wir

$$S_2^*(n) = \sum_{x_2 < p \leqq n}^{(1)} \omega_{x_2}(f(p)) + \sum_{x_2 < p \leqq n}^{(2)} \omega_{x_2}(f(p)),$$

und wir entscheiden folgendermaßen, ob wir p zur ersten oder zur zweiten Summe zählen: Es sei Πq^α die Darstellung von $f(p)$ als Produkt von Primzahlpotenzen. Dann setzen wir p in die erste Summe, wenn das entsprechende Teilprodukt $\prod_{q < x_2} q^\alpha \geqq n^{1/2}$, und in die zweite Summe, wenn $\prod_{q < x_2} q^\alpha < n^{1/2}$ ist.

Man kann ziemlich leicht zeigen[12]), daß die Anzahl derjenigen m, $m \leqq n$, für die, wenn man die Primfaktorzerlegung von $f(m)$ mit Πq^α bezeichnet, $\prod_{q < x_2} q^\alpha \geqq n^{1/2}$ gilt, gleich $o(n\mu^{-2})$ ist. Daher erhalten wir aus (10) die Gleichung

$$S(n) = \sum_{x_2 < p \leqq n}^{(2)} \omega_{x_2}(f(p)) + O(n\mu^{-1}\nu^{1/2}). \tag{11}$$

---

[11]) *A. Selberg*, Norske Vid. Selsk. Forh., Trondhjem **19**, No. 18 (1947), 64—67.

[12]) Methode von *P. Erdös*, J. London Math. Soc. **27** (1952), 7—15, Lemmas 1, 5, 6.

Endlich knüpfen wir an die ursprüngliche Hardy-Ramanujan Methode an. Man schreibt (11) in der Form

$$S(n) - \{1 + o(1)\} n \nu \mu^{-1} = \sum_{\substack{x_3 < p \leq n \\ |\omega_{x_3}(f(p)) - \nu| > \varepsilon\nu}}^{(2)} \{\omega_{x_3}(f(p)) - \nu\} = O\Big(\sum_{\substack{k \\ |k-\nu| > \varepsilon\nu}} |k - \nu| \, G_k(n)\Big), \quad \varepsilon = o(1),$$

wo $G_k(n)$ die Anzahl derjenigen Primzahlen $p, x_3 < p \leq n$, ist, für die $f(p)$ genau k verschiedene Primteiler $q_1, \ldots, q_k$ $(q_i < x_2, q_i \nmid f(0), (i = 1, 2, \ldots, k); q_1^{\alpha_1} \cdots q_k^{\alpha_k} \leq n^{1/2})$ hat. Wir benutzen wieder die Selbergsche Siebmethode und beweisen damit, daß

$$G_k(n) \leq c_5 \left\{ \frac{1}{k!} \frac{n}{\mu^3} (\nu + c_6)^{k+c_7} + n^{\frac{1}{2} + \frac{2}{\nu^2}} \mu^7 \right\}$$

und folglich

$$\sum_{\substack{k \\ |k-\nu| > \varepsilon\nu}} |k - \nu| \, G_k(n) \leq c_8 \frac{n}{\mu^3} \nu^{c_7+1} \sum_{\substack{k \\ |k-\nu| > \varepsilon\nu}} \frac{(\nu + c_6)^{k-1}}{(k-1)!} + O(n\mu^{-2})$$

ist. Nun aber kann man zeigen (Erdös [7]), Seite 209), daß

$$n\mu^{-2} \nu^{c_7+1} \sum_{\substack{k \\ |k-\nu| > \varepsilon\nu}} \frac{(\nu + c_6)^{k-1}}{(k-1)!} = O(n\mu^{-1-\delta}),$$

ist, wo δ eine gewisse, von ε abhängige positive Zahl bedeutet, und somit ist der Beweis von Satz 3 beendet.

University College, Exeter.

Eingegangen 10. Februar 1955.

Erweiterungsproblem galoisscher Körper und Zerfall einfacher Algebren.

Von *Gudrun Beyer* in Hamburg.

Einen Zusammenhang zwischen dem Zerfall einfacher Algebren und der Lösbarkeit gewisser Erweiterungsprobleme galoisscher Körper hat zuerst R. Brauer [2] festgestellt. Hasse [4] zeigte, daß umgekehrt jedes Erweiterungsproblem galoisscher Körper (bei abelscher Relativgruppe $\mathfrak{N}$) mit der Frage nach dem Zerfall gewisser einfacher Algebren zusammenhängt. Der Zusammenhang wurde übersichtlicher dadurch, daß diese einfachen Algebren zu einer halbeinfachen Algebra G, dem „verschränkten Gruppenring" des Erweiterungsproblems [10] zusammengefaßt wurden. Es interessiert dann der Zerfall von G über ihrem Zentrum (oder das Einswerden ihrer Schurschen Indizes). Delone-Faddeev [3] fanden diesen Zusammenhang auf anderem Wege. Alle genannten Autoren beschränkten sich auf abelsche Relativgruppen $\mathfrak{N}$ im Erweiterungsproblem. P. Wolf [10] konnte bei nichtabelschem $\mathfrak{N}$ einen ähnlichen Zusammenhang zwischen Erweiterungsproblem und „Zerfall" des verschränkten Gruppenringes G feststellen, wobei er aber einen anderen Zerfallsbegriff zugrundelegt. Es soll hier dieser Begriff auf einen bekannten Zerfallsbegriff (Jehne [6]) zurückgeführt werden, der insbesondere, wenn $\mathfrak{N}$ abelsch ist oder wenn der betrachtete galoissche Körper Ω/Ω_0 die absolut irreduziblen Charaktere von $\mathfrak{N}$ enthält, gerade auf den Zerfall der Algebra G über ihrem Zentrum hinausläuft.

Die dazu benötigte Strukturuntersuchung von G ist nach Nakayama-Shoda [7] auch für die Theorie der Darstellungen endlicher Gruppen durch halblineare Transformationen von Interesse. Sie gestattet ferner als Nebenresultat einen neuen Beweis eines gewissen Einzigkeitssatzes [1].

1. Es sei Ω/Ω_0 ein galoisscher Körper mit der Gruppe $\mathfrak{g}$, die zugleich als Faktorgruppe der endlichen Gruppe $\mathfrak{G}$ mit dem Kern $\mathfrak{N}$ dargestellt und mit dieser identifiziert sei. Die Charakteristik von Ω gehe nicht in der Ordnung von $\mathfrak{N}$ auf. Das *Erweiterungsproblem* von Ω/Ω_0 mit $\mathfrak{G}$ besteht in der Frage nach einer kommutativen galoisschen Algebra K/Ω mit der Gruppe $\mathfrak{N}$, die zugleich über Ω_0 mit der Gruppe $\mathfrak{G}$ galoissch ist. Dabei heißt eine kommutative Algebra K/Ω_0 *galoissch mit der Gruppe* $\mathfrak{G}$, wenn sie halbeinfach ist, $\mathfrak{G}$ als Automorphismengruppe über Ω_0 besitzt und eine der beiden folgenden, zueinander äquivalenten Eigenschaften hat:

a) K besitzt über dem Grundkörper Ω_0 eine Normalbasis bezüglich $\mathfrak{G}$ (d. h. eine Basis, die aus den $\mathfrak{G}$-Konjugierten eines Elementes besteht),

b) $\mathfrak{G}$ läßt nur den Grundkörper Ω_0 elementweise fest, und der Rang von K/Ω_0 ist mindestens gleich der Ordnung von $\mathfrak{G}$:

$$[K:\Omega_0] \geqq (\mathfrak{G}:1).$$

Eine kommutative galoissche Algebra ist direkte Summe zueinander isomorpher und unter $\mathfrak{G}$ konjugierter galoisscher Körper.

Eine beliebige Algebra L/Ω_0 heißt (nach Jehne [6]) *galoissch mit der Gruppe* $\mathfrak{G}$, wenn ihr Zentrum K eine kommutative galoissche Algebra über Ω_0 mit der Gruppe $\mathfrak{G}$ ist und die Galois-Automorphismen von K sich auf die volle Algebra L fortsetzen lassen (wenn also, anders gesagt, $\mathfrak{G}$ äußere Automorphismengruppe von L/Ω_0 ist, die im Zentrum eine Galoisgruppe induziert). Teichmüller und Jehne [6] haben für solche Algebren eine Theorie der verschränkten Produkte entwickelt. Insbesondere ist ein verschränktes Produkt von L/Ω_0 mit einer Galoisgruppe eine zentrale einfache Algebra über Ω_0 und ist in ihm L die Gesamtheit aller mit K elementweise vertauschbaren Elemente.

Auf die in der Einleitung genannte Algebra G/Ω_0, die dem Erweiterungsproblem zugeordnet ist, führt der folgende Gedankengang. Angenommen, das Erweiterungsproblem ist lösbar durch eine galoissche Algebra K/Ω_0. Dann betrachte man das verschränkte Produkt von K/Ω_0 mit der Galoisgruppe $\mathfrak{G}$ zum Faktorensystem 1. Beschränkt man in der Darstellung

$$\sum_{S \text{ aus } \mathfrak{G}} S\alpha_S \qquad (\alpha_S \text{ aus } K)$$

seiner Elemente die Koeffizienten α_S auf Ω, so erhält man eine Algebra G, die ohne Kenntnis der Erweiterungsalgebra K konstruiert werden kann. Diese Algebra G/Ω_0, *der verschränkte Gruppenring* von $\mathfrak{G}$ über Ω/Ω_0, ist also definiert als die Ω enthaltende Algebra über Ω_0 mit einer Relativbasis über Ω, die sich zur Gruppe $\mathfrak{G}$ isomorph multipliziert und mit dieser identifiziert werden möge, also mit dem allgemeinen Element

$$\sum_{S \text{ aus } \mathfrak{G}} Sa_S \text{ mit } a_S \text{ aus } \Omega,$$

und mit der Vertauschungsregel

$$aS = Sa^s \text{ für } a \text{ in } \Omega \text{ und } s = S \bmod \mathfrak{N}.$$

In den extremen Spezialfällen $\mathfrak{g} = 1$ bzw. $\mathfrak{N} = 1$ ist G der Gruppenring von $\mathfrak{N}$ über Ω bzw. das verschränkte Produkt von Ω/Ω_0 mit seiner Galoisgruppe zum Faktorensystem 1.

2. Der verschränkte Gruppenring G enthält den wegen der Charakteristikvoraussetzung halbeinfachen Gruppenring N von $\mathfrak{N}$ über Ω in Form der Elemente

$$\sum_{U \text{ aus } \mathfrak{N}} Ua_U.$$

Die direkte Zerlegung von N in einfache Ideale sei

$$N = \operatorname{dir} \sum_{\chi} e_\chi N,$$

wobei die e_χ die unzerlegbaren Zentrumsidempotente von N in bekannter Zuordnung zu den über Ω irreduziblen Charakteren χ von $\mathfrak{N}$ bedeuten. Da $\mathfrak{N}$ Normalteiler in $\mathfrak{G}$ ist, sind die Relativbasiselemente S von G über Ω mit dem Gruppenring N als Ganzem vertauschbar, so daß N bei den durch Transformation mit den S bewirkten inneren Automorphismen von G insgesamt invariant ist, also Automorphismen erfährt. Diese durch Transformation mit den S aus $\mathfrak{G}$ gelieferten Automorphismen von N lauten explizit

$$\Big(\sum_{U \text{ aus } \mathfrak{N}} Ua_U\Big)^S = S^{-1}\Big(\sum_{U \text{ aus } \mathfrak{N}} Ua_U\Big) S = \sum_{U \text{ aus } \mathfrak{N}} U^S a_U^s,$$

wo wie in allem Folgenden $s = S \bmod \mathfrak{N}$ und $U^S = S^{-1}US$ bedeutet. Die im Zentrum C von N induzierten Automorphismen hängen nur von den zugeordneten Elementen s aus $\mathfrak{g} = \mathfrak{G}/\mathfrak{N}$ ab und stimmen im Teilkörper Ω mit den Galois-Automorphismen überein. Sie seien demgemäß mit den Exponenten s bezeichnet. Insbesondere werden bei diesen Automorphismen die Zentrumsidempotente e_χ von N untereinander permutiert:

$$e_\chi^s = e_{\chi_s}.$$

Dies definiert eine zu $\mathfrak{g}$ homomorphe Gruppe Γ von Permutationen $\chi \to \chi_s$ der Charaktere χ. Die Klassen Γ-konjugierter Charaktere (Transitivitätsgebiete unter Γ) mögen mit $\mathfrak{K}$ bezeichnet werden. Γ-konjugierte Charaktere haben gleichen Grad, denn die ihnen entsprechenden einfachen Ideale des Gruppenringes gehen durch die Automorphismen S von N auseinander hervor, sind also als Algebren über Ω_0 isomorph (als Algebren über Ω nur halblinear isomorph).

3. Die den Charakterklassen $\mathfrak{K}$ zugeordneten orthogonalen Idempotente $e_{\mathfrak{K}} = \sum_{\chi \text{ in } \mathfrak{K}} e_\chi$ des verschränkten Gruppenringes haben die Eigenschaft $\sum_{\mathfrak{K}} e_{\mathfrak{K}} = 1$. Sie liegen sicherlich im Zentrum Z von G und gestatten jedenfalls innerhalb N keine weitere Zerlegung in orthogonale Zentrumsidempotente von G. Im folgenden Satz wird darüber hinaus gezeigt, daß die $e_{\mathfrak{K}}$ sogar innerhalb G im Zentrum orthogonal unzerlegbar sind.

Daß die Algebra G halbeinfach ist (Nakayama-Shoda [7], Osima [8]), folgt aus der weitergehenden Aussage, daß das Ideal $e_{\mathfrak{K}}G$ einfach ist. Diese Aussage ist in dem folgenden Satz enthalten, den unter der Voraussetzung, daß $\mathfrak{N}$ abelsch ist und Ω die absolut irreduziblen Charaktere von $\mathfrak{N}$ enthält, Hasse [4] bewiesen hat.

Satz. a) *In der direkten Zerlegung*

$$N = \operatorname{dir} \sum_{\mathfrak{K}} N_{\mathfrak{K}}, \quad N_{\mathfrak{K}} = e_{\mathfrak{K}} N = N e_{\mathfrak{K}}$$

des Gruppenringes N von $\mathfrak{N}$ über Ω nach den Charakterklassen $\mathfrak{K}$ von $\mathfrak{N}$ über Ω hat bei der Automorphismengruppe $\mathfrak{G}$ von N jeder Bestandteil $N_{\mathfrak{K}}$ als Invarianzteilalgebra einen Erweiterungskörper $Z_{\mathfrak{K}}/e_{\mathfrak{K}}\Omega_0$, und es ist $N_{\mathfrak{K}}$ eine galoissche Algebra mit der (Faktor-) Gruppe $\mathfrak{g}$ über $Z_{\mathfrak{K}}$. Ihr Zentrum $C_{\mathfrak{K}}$ ist dabei galoissch vom Typus

$$C_{\mathfrak{K}} = Z_{\mathfrak{K}} \times e_{\mathfrak{K}}\Omega.$$

b) *In der direkten Zerlegung*

$$G = \operatorname{dir} \sum_{\mathfrak{K}} G_{\mathfrak{K}} \text{ mit } G_{\mathfrak{K}} = e_{\mathfrak{K}} G = G e_{\mathfrak{K}}$$

des verschränkten Gruppenringes G von $\mathfrak{G}$ über Ω/Ω_0 vermöge der orthogonalen Zentrumsidempotente $e_{\mathfrak{K}}$ ist jeder Bestandteil $G_{\mathfrak{K}}$ ein verschränktes Produkt der galoisschen Algebra $N_{\mathfrak{K}}$ mit ihrer Gruppe $\mathfrak{g}$. Ist nämlich

$$\mathfrak{G} = \bigcup_s R_s \mathfrak{N}, \quad R_s R_t = R_{st} Q_{s,t} \; (Q_{s,t} \text{ in } \mathfrak{N})$$

eine Zerlegung von $\mathfrak{G}$ nach $\mathfrak{N}$, so bilden die

$$r_s = e_{\mathfrak{K}} R_s$$

eine Relativbasis von $G_{\mathfrak{K}}$ über $N_{\mathfrak{K}}$ mit den Relationen

$$\alpha r_s = r_s \alpha^{R_s} \; (\alpha \text{ in } N_{\mathfrak{K}}), \quad r_s r_t = r_{st} q_{s,t} \quad (q_{s,t} = e_{\mathfrak{K}} Q_{s,t}),$$

also mit dem Faktorensystem $q_{s,t}$.

c) *Insbesondere ist demnach jeder Bestandteil $G_{\mathfrak{K}}$ einfach (mit $Z_{\mathfrak{K}}$ als Zentrum) und somit G selbst halbeinfach.*

Beweis. a) Die durch die inneren Automorphismen S aus $\mathfrak{G}$ von G im Zentrum $C_{\mathfrak{K}}$ von $N_{\mathfrak{K}}$ induzierten Automorphismen bilden eine zu $\mathfrak{g}$ homomorphe Gruppe. Diese ist sogar zu $\mathfrak{g}$ isomorph, weil im Teilkörper $e_{\mathfrak{K}}\Omega$ alle Automorphismen s voneinander verschieden sind. Der Invarianzring $Z_{\mathfrak{K}}$ von $C_{\mathfrak{K}}$ bei dieser Gruppe ist ein Körper, weil bei ihr alle Idempotente e_χ (χ in $\mathfrak{K}$) transitiv permutiert werden.

Das Kompositum P der beiden Teilkörper $Z_{\mathfrak{K}}$ und $e_{\mathfrak{K}}\Omega$ von $C_{\mathfrak{K}}$ besitzt als Algebra über $Z_{\mathfrak{K}}$ die Automorphismengruppe $\mathfrak{g}$, die in $e_{\mathfrak{K}}\Omega$ die Galoisgruppe über $e_{\mathfrak{K}}\Omega_0$ induziert. Wegen seiner Kommutativität ist P also ring- und $\mathfrak{g}$-homomorphes Bild des über $e_{\mathfrak{K}}\Omega_0$

$$\begin{tikzcd}
 & G_{\mathfrak{K}} = \sum_{\mathfrak{K}} r_s N_{\mathfrak{K}} \arrow[d, dash] \\
 & N_{\mathfrak{K}} \arrow[d, dash] \\
 & C_{\mathfrak{K}} = Z_{\mathfrak{K}} \times e_{\mathfrak{K}}\Omega \arrow[dl, dash, "\mathfrak{g}"'] \arrow[d, dash, "\mathfrak{g}"] \\
e_{\mathfrak{K}}\Omega \arrow[r, dash] & Z_{\mathfrak{K}} \\
e_{\mathfrak{K}}\Omega_0 \arrow[u, dash, "\mathfrak{g}"] \arrow[ur, dash] &
\end{tikzcd}$$

genommenen direkten Produktes $D = Z_{\mathfrak{K}} \times e_{\mathfrak{K}}\Omega$. Dieses ist als Ringerweiterung des galoisschen Körpers $e_{\mathfrak{K}}\Omega/e_{\mathfrak{K}}\Omega_0$ galoissche Algebra mit der Gruppe $\mathfrak{g}$ über $Z_{\mathfrak{K}}$. Als solche enthält D aber kein eigentliches, bei $\mathfrak{g}$ zulässiges Ideal, also ist P sogar isomorph zu D:

$$P = Z_{\mathfrak{K}} \times e_{\mathfrak{K}}\Omega .$$

Da P in $C_{\mathfrak{K}}$ enthalten ist, folgt hieraus insbesondere, daß die nur den Grundkörper invariant lassende Automorphismengruppe $\mathfrak{g}$ der halbeinfachen kommutativen Algebra $C_{\mathfrak{K}}/Z_{\mathfrak{K}}$ eine Ordnung hat, die höchstens gleich dem Rang dieser Algebra ist. Demnach ist $C_{\mathfrak{K}}$ bei dieser Gruppe $\mathfrak{g}$ galoissch und stimmt aus Ranggründen mit P überein. Die Galois-Automorphismen von $C_{\mathfrak{K}}$ lassen sich offenbar fortsetzen zu Automorphismen von $N_{\mathfrak{K}}$.

b) Die Elemente $r_s = e_{\mathfrak{K}} R_s$ aus $G_{\mathfrak{K}}$ genügen sicherlich den im Satz genannten Relationen. Daraus folgt, daß $G_{\mathfrak{K}}$ ringhomomorphes Bild des verschränkten Produktes von $N_{\mathfrak{K}}$ mit $\mathfrak{g}$ zum Faktorensystem $q_{s,t}$ ist, dessen Assoziativität aus der Assoziativität von $Q_{s,t}$ folgt. Da dieses verschränkte Produkt eine einfache Algebra ist, muß $G_{\mathfrak{K}}$ sogar ringisomorphes Bild derselben sein. Insbesondere bilden demnach die r_s eine Relativbasis von $G_{\mathfrak{K}}$ über $N_{\mathfrak{K}}$.

c) Die letzte Aussage des Satzes folgt dann unmittelbar aus der Theorie der verschränkten Produkte. (Die in [6] gemachte Voraussetzung, daß Ω unendlich sein soll, ist nach M. Kneser unwesentlich.)

4. Wie Delone-Faddeev [3] und unabhängig von ihnen Hasse [4] und Wolf [9] gezeigt haben, ist notwendig für die Lösbarkeit des Erweiterungsproblems die Existenz eines *Verkettungssystems*, d. h. eines Systems von regulären Elementen des Gruppenringes N, die den Gleichungen

$$(\mathfrak{B}) \qquad B_{st} Q_{s,t} = B_t B_s^{R_t}$$

genügen. Im Hinblick auf die Einbettung des Gruppenringes N in den verschränkten Gruppenring G bezeichnete Wolf [10] die Lösbarkeit dieser Gleichungen ($\mathfrak{B}$) mit „*Zerfall des verschränkten Gruppenringes G*". Dieser Zerfall hat durch den in Nr. 3 bewiesenen Satz eine neue Bedeutung gewonnen: Er ist *gleichbedeutend mit dem Zerfall im Sinne der Theorie der verschränkten Produkte* der Faktorensysteme $q_{s,t}$ der sämtlichen im Satz genannten verschränkten Produkte $G_{\mathfrak{K}}$ der $N_{\mathfrak{K}}$. Zerfällt der Gruppenring N über seinem Zentrum, so ist dies (Jehne [6], S. 82f.) gleichbedeutend mit dem *Zerfall der halbeinfachen Algebra G*

über ihrem Zentrum. Das ist also z. B. der Fall, wenn $\mathfrak{N}$ abelsch ist oder wenn Ω die absolut irreduziblen Charaktere von $\mathfrak{N}$ enthält. Im allgemeinen kann man nur aussagen, daß der Exponent der einfachen Algebra $G_{\mathfrak{K}}$ mit demjenigen von $e_\chi N$ (χ aus $\mathfrak{K}$) übereinstimmt, wenn das zugehörige Faktorensystem $q_{s,t}$ zerfällt. (Ist Ω endlich algebraischer Zahlkörper, so ist er jedenfalls ein Vielfaches des letzteren, auch wenn $q_{s,t}$ nicht zerfällt.)

Die bekannte Reduktion [6] der Theorie der verschränkten Produkte einer halbeinfachen galoisschen Algebra auf die Theorie der verschränkten Produkte einer einfachen galoisschen Algebra gestattet weiter auch hier ein Analogon der bei Hasse [4] durchgeführten Reduktion der Gleichungen ($\mathfrak{B}$). Insbesondere ergibt sich ein neuer Beweis einer von Osima ([8], Satz 6 und 7) gefundenen Tatsache über Darstellungen endlicher Gruppen durch halblineare Transformationen, der unter der Voraussetzung, daß der Grundkörper Ω_0 die absolut irreduziblen Charaktere von $\mathfrak{N}$ enthält, in ähnlicher Weise von Nakayama-Shoda ([7], Satz 5) geführt wurde.

5. Daß es „im wesentlichen" nur ein Verkettungssystem für ein Erweiterungsproblem geben kann, hat Hasse [4], [5] unter der Voraussetzung bewiesen, daß $\mathfrak{N}$ abelsch ist und Ω die absolut irreduziblen Charaktere von $\mathfrak{N}$ enthält. Den ersten, rechnerischen, seiner beiden Beweise, der die Unendlichkeit von Ω zur Voraussetzung hat, habe ich früher [1] für den hier betrachteten Fall verallgemeinert. Mit Hilfe des Satzes aus Nr. 3 läßt sich nunmehr auch der zweite, begriffliche, Beweis von Hasse übertragen, so daß der Satz insbesondere von der Unendlichkeitsvoraussetzung für Ω befreit ist. Es gilt also:

Einzigkeitssatz. *Sind B_s und B'_s Lösungen von ($\mathfrak{B}$) im Gruppenring N, so gibt es ein reguläres A in N derart, daß*

$$AB'_s = B_s A^{R_s}$$

ist.

Beweis. Daß das System B_s aus N den Gleichungen ($\mathfrak{B}$) genügt, ist gleichbedeutend damit, daß die Elemente

$$V_s = R_s B_s^{-1} \tag{1}$$

aus dem verschränkten Gruppenring G die Eigenschaft

$$V_{st} = V_s V_t \tag{2}$$

haben. Die Gleichungen (1) besagen, daß der durch Transformation mit V_s bewirkte Automorphismus von N derselben äußeren Automorphismenklasse angehört wie R_s oder daß im Zentrum C von N

$$V_s^{-1}\tilde{A}V_s = \tilde{A}^s \text{ für } \tilde{A} \text{ aus } C$$

gilt. Für die einzelnen Komponenten $e_{\mathfrak{K}}G$ bedeutet dies, daß die $e_{\mathfrak{K}}V_s$ ($s \in \mathfrak{g}$) über der galoisschen Algebra $C_{\mathfrak{K}}$ das verschränkte Produkt P mit Faktorensystem 1 erzeugen. Gibt es also ein zweites B'_s, d. h. ein V'_s und somit $V'_s e_{\mathfrak{K}}$ und P' mit den entsprechenden Eigenschaften, so sind P und P' über $C_{\mathfrak{K}}$ isomorphe einfache Teilalgebren der einfachen Algebra $e_{\mathfrak{K}}G$, und es gibt einen inneren Automorphismus von $e_{\mathfrak{K}}G$, der $C_{\mathfrak{K}}$ elementweise fest läßt und $e_{\mathfrak{K}}V_s$ in $e_{\mathfrak{K}}V'_s$ überführt. Sei $A_{\mathfrak{K}}$ ein zugehöriger Transformator:

$$(3_1)\quad A_{\mathfrak{K}}^{-1}\tilde{A}A_{\mathfrak{K}} = \tilde{A} \text{ für } \tilde{A} \text{ aus } C_{\mathfrak{K}} \qquad (3_2)\quad A_{\mathfrak{K}}^{-1}e_{\mathfrak{K}}V_s A_{\mathfrak{K}} = e_{\mathfrak{K}}V'_s\,.$$

Nach der Theorie der verschränkten Produkte muß wegen (3_1) $A_{\mathfrak{K}}$ in $N_{\mathfrak{K}}$, also

$$A = \sum_{\mathfrak{K}} A_{\mathfrak{K}}$$

im Gruppenring N liegen. Wegen (3_2) ist

$$A^{-1} V_s A = V'_s,$$

also nach (1)

$$A B'_s = B_s A^{R_s}.$$

Damit ist der Einzigkeitssatz neu bewiesen.

Literatur.

[1] *G. Beyer*, Ein Einzigkeitssatz in der Einbettungstheorie galoisscher Körper, Math. Nachr. **11**, 317—320 (1954).

[2] *R. Brauer*, Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind. J. reine angew. Math. **168**, 44—64 (1932).

[3] *D. K. Delaunay* and *B. N. Faddeieff* (*Delone* und *Faddeev*), Investigations in the geometry of the Galois theory [russ. mit engl. Zs.fssg.]. Mat. Sbornik, n. Ser. **15**, 243—284 (1944), insbes. S. 272.

[4] *H. Hasse*, Existenz und Mannigfaltigkeit abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers. I. Math. Nachr. **1**, 40—61 (1948).

[5] *H. Hasse*, Invariante Kennzeichnung relativ abelscher Zahlkörper mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers. Abh. Deutsche Akad. Wiss. Berlin, math. naturw. Kl. **1947**, Nr. 8 (1949), insbes. S. 32.

[6] *W. Jehne*, Idelklassenfaktorensysteme und verallgemeinerte Theorie der verschränkten Produkte. Abh. math. Sem. Univ. Hamburg **18**, 70—98 (1952).

[7] *T. Nakayama* und *K. Shoda*, Über die Darstellung einer endlichen Gruppe durch halblineare Transformationen. Japan. J. Math. **12**, 109—122 (1936).

[8] *M. Osima*, Über die Darstellung einer endlichen Gruppe durch halblineare Transformationen. Proc. phys. math. Soc. Japan **20**, 1—5 (1938).

[9] *P. Wolf*, Galoissche Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers. I. Math. Nachr. **9**, 281—300 (1953).

[10] *P. Wolf*, Das Einbettungsproblem galoisscher Algebren. J. reine angew. Math. **193**, 166—182 (1954), insbes. S. 177f.

Eingegangen 4. Mai 1955.

(1954).
gebenes
theory
einem
einem
(1949),
. math.
sforma-
. phys.
pers. I,
insbes.